User's ▶▶▶▶▶ Manual

Dual WAN 4-Port Firewall Router

H2BR4

Trademarks & Copyright

Windows 95/98/ME and Windows NT/2000/XP are registered trademarks of Microsoft Corp. All other brands and product names are trademarks of their respective companies.

No part of this publication may be reproduced in any form or by any means or used to make any derivative (such as translation, transformation or adaptation) without the express written consent of the manufacturer as stipulated by the United States Copyright Act of 1976.

FCC Certifications

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures. All trademarks and brand names are the property of their respective proprietors. Specifications are subject to change without prior notification.

HAWKING LIMITED WARRANTY

Hawking Technology guarantees that every H-BR49 Broadband Router is free from physical defects in material and workmanship under normal use for two (2) years from the date of purchase. If the product proves defective during this two-year warranty period, call Hawking Customer Service in order to obtain a Return Authorization number. Warranty is for repair or replacement only. Hawking Technology does not issue any refunds. BE SURE TO HAVE YOUR PROOF OF PURCHASE. RETURN REQUESTS CAN NOT BE PROCESSED WITHOUT PROOF OF PURCHASE. When returning a product, mark the Return Authorization number clearly on the outside of the package and include your original proof of purchase.

IN NO EVENT SHALL HAWKING TECHNOLOGY'S LIABILTY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE OR ITS DOCUMENTATION. Hawking Technology makes no warranty or representation, expressed, implied or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Hawking Technology reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to: techsupport@hawkingtech.com.

Table of Contents

H2BR4 Dual WAN 4-Port Firewall Router

Package Contents

H2BR4 Dual WAN 4-Port Firewall Router

The complete H2BR4 package consists of:

- One H2BR4 Dual WAN 4-Port Firewall Router
- One Quick Installation Guide
- One CD with User's Manual
- One Power Adapter
- Accessories

Check to make sure that the unit was not damaged during shipping and that no items are missing. If you encounter a problem, please contact your dealer.

Please read this manual thoroughly, and follow the installation and operation procedures detailed in this user's manual.

The high performance Hawking H2BR4 Dual WAN Firewall Router with built-in 4-port 10/100M Ethernet Switch provides an easy-to-use, cost-effective means of sharing two broadband Internet connections with your LAN (Local Area Network). With the H2BR4's two WAN ports, users experience significantly faster data rates as a result of increased and more efficient use of bandwidth. The dual WAN ports also provide: an easy way to utilize two different types of broadband Internet connections on the same network (i.e., DSL, Cable, T1, etc.), a method for selectively managing traffic between Internet connections (i.e., by port or IP address), and a back-up method that activates the second WAN if the first WAN should get disconnected.

The H2BR4 features high-level security and is equipped with true, hardware-based firewall protection. The firewall utilizes Stateful Packet Inspection (SPI) technology, Network Address Translation, and prevents against Denial of Service (DoS) attacks from outside intruders. In addition, the VPN (Virtual Private Network) pass-through feature allows for fast, reliable, and secure access to your corporate network via a public Internet network.

The H2BR4 includes a full set of powerful features. It utilizes Network Address Translation (NAT) to expand your existing network without affecting existing IP based account schemes. The router supports DSL, Cable, and other broadband modem connections that connect to an RJ-45 Ethernet port. The H2BR4 also features Virtual Server and DMZ functions, which allow the user to protect clients on the network behind the router while permitting specified traffic to be opened up outside the network. The router has a built-in DHCP server, which eliminates the need to configure each IP address manually. The user-friendly web management interface provides the user with an easy way to configure the router from anywhere in the world using a web browser. The H2BR4 can easily be firmware upgraded and is compatible with all standard Internet applications. It provides a complete solution for small/medium business and small office/home office users.

Features
- Superb throughput of up to 50Mbps
- Allows multiple users to share a single Internet line or two Internet lines
- Supports up to 253 users
- Internet Access via Cable or xDSL modem
- Can Access Private LAN Servers from the Public Network
- Equipped with two WAN ports (10/100M) and four LAN ports (10/100M)
- Supports DHCP (Server/Client) for easy setup
- Supports advanced features such as:
    - Special Applications (i.e., Port Triggers, etc.)
    - DMZ
    - Virtual Servers
    - Network Access Control
    - Firewall
    - Bridge mode
    - DDNS (DynDNS/TZO)
    - Content Filtering
- Allows you to monitor the router's status via: DHCP Client Log, Security Log and Device/Connection Status
- Easy-to-use Web-based user interface for configuration and management purposes
- Remote management allows configuration and upgrades from a remote site (over the Internet)

Minimum Requirements

- One External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45)
- Network Interface Card (NIC) for each Personal Computer (PC)
- PCs with a Web-Browser (Internet Explorer 4.0 or higher, or Netscape Navigator 4.7 or higher)

<u>*Note*</u>

The WAN "idle timeout" auto-disconnect function may not work due to abnormal activities of some network application software, computer viruses or hacker attacks from the Internet. For example, some types of software send network packets to the Internet in the background, even when you are not using the Internet. This function also may not work with some ISPs. Please make sure this function works properly when you use this function for the first time, especially if your ISP charges you according to time used. Due to such issues, we cannot guarantee that the WAN "idle timeout" auto-disconnect function will work in all situations. In order to prevent an extra fee from being charged by the ISP, if your ISP uses such a fee structure, please *turn off the router when you are finished using the Internet*.

Get to Know the Broadband Router

Back Panel

The diagram below (Figure 1.0) shows the router's back panel. The router's back panel is divided into three sections, LAN, WAN and Reset:
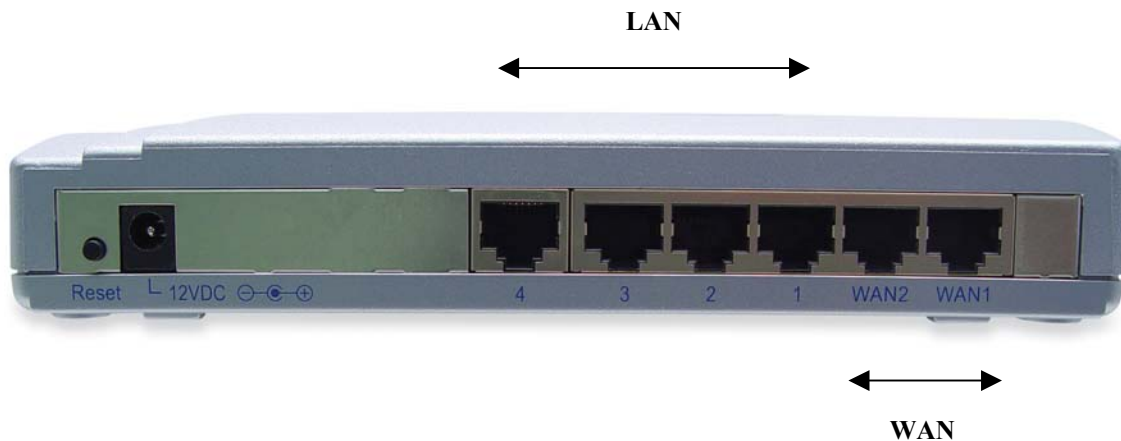

Figure 0.0

Introduction
H2BR4 Dual WAN 4-Port Firewall Router

1) *Local Area Network (LAN)*
   The router's four LAN ports are what you will use to connect your PCs, print servers, switches, etc.

2) *Wide Area Network (WAN)*
   The WAN ports are the segments that connect to your xDSL or Cable modems and are linked to the Internet.

3) *Reset*
   The Reset button allows you to do one of two things:

      i.   If problems occur with your router, press the router's reset button with a narrow pen tip (for less than four seconds) and the router will re-boot itself, keeping your original configurations.

      ii.   If problems persist or become serious, or if you forget your password, press the reset button for longer than four seconds and the router will reset itself to the factory default settings. **Warning**: Your original configurations will be replaced with the factory default settings.

Front Panel

The LED lights located on the router's front/top panel provide you with information on the device's status at any given time. Below is a detailed description of the LEDs.

Figure 0.1

LED	Light Status	Description
PWR	ON	Router's power supply is on
WAN 10/100M (Port 1-2)	ON	100Mbps connection
	Off	10Mbps connection
WAN LNK/ACT (Port 1-2)	ON	WAN is connected
	Off	No WAN connection
	Flashing	WAN port has Activity (ACT); data being sent
LAN 10/100M (Port 1-4)	ON	100Mbps connection
	Off	10Mbps connection
LAN LNK/ACT (Port 1-4)	ON	LAN is connected
	Off	No LAN connection
	Flashing	LAN port has Activity (ACT); data being sent

Setup Diagram

Figure 1.2 below shows a typical setup for a Local Area Network (LAN).
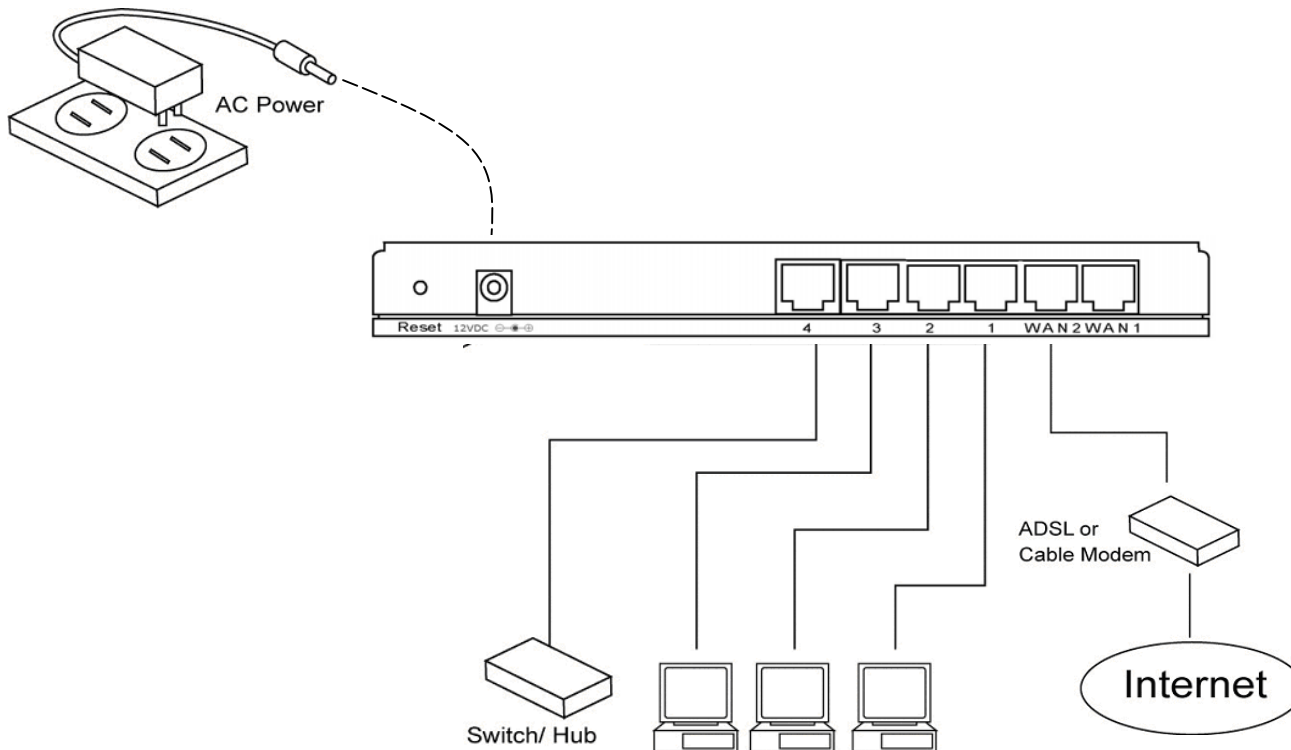

Figure 0.2

Getting started

The following are step-by-step instructions on how to start using the router and get connected to the Internet.

1)   Set up your network as shown in the setup diagram above (Figure 1.2).

2)   You then need to set your LAN PC clients so that they can obtain an IP address automatically. All LAN clients require an IP address. Just like a street address, it allows LAN clients to find one another. (If you have already configured your PC to obtain an IP address automatically then proceed to step 3, page 11.)

Configure your PC to obtain an IP address automatically

By default, the router's DHCP is on (enabled). This means that you can obtain an IP address automatically once you've configured your *PC* to obtain an IP address automatically. This section will show you how to configure your PC so that it can obtain an IP address automatically for either Windows 95/98/Me, 2000 or NT operating

systems. For other operating systems (Macintosh, Sun, etc.), follow the manufacturer's instructions. The following is a step-by-step illustration on how to configure your PC to obtain an IP address automatically for: 2a) **Windows 95/98/Me**, 2b) **Windows 2000** and 2c) **Windows NT**.

2a) Windows 95/98/Me

i: Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.

ii: Double-click *Network* icon. The *Network* window will appear.

iii: Check your list of Network Components. If TCP/IP is not installed, click the *Add* button to install it now. If TCP/IP is installed, go to **step 6**.

iv: In the *Network Component Type* dialog box, select *Protocol* and click *Add* button.

v: In the *Select Network Protocol* dialog box, select *Microsoft* and *TCP/IP* and then click the *OK* button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.

vi: After installing TCP/IP, go back to the *Network* dialog box. Select *TCP/IP* from the list of *Network Components* and then click the *Properties* button.

vii: Check each of the tabs and verify the following settings:

- **Bindings**: Check *Client for Microsoft Networks* and *File and printer sharing for Microsoft Networks*.
- **Gateway**: All fields are blank.
- **DNS Configuration**: Select *Disable DNS.*
- **WINS Configuration**: Select *Disable WINS Resolution.*
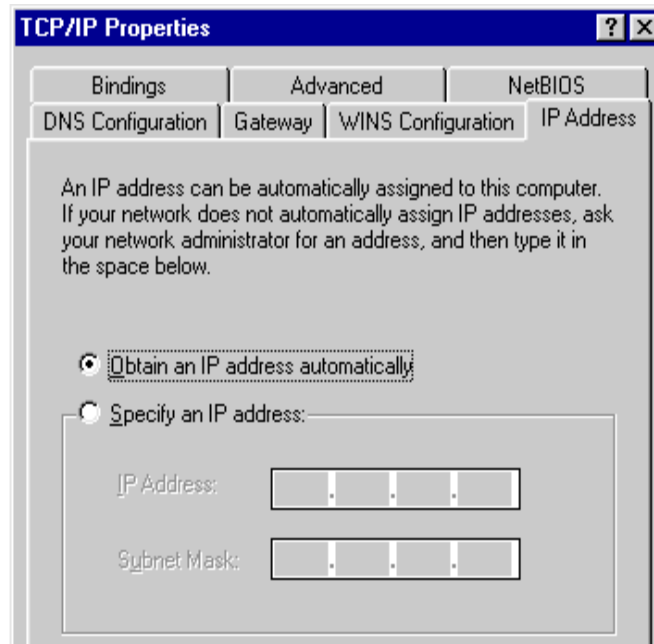- **IP Address**: Select *Obtain IP address automatically*.

Figure 0.3

viii: Reboot the PC. Your PC will now obtain an IP address automatically from your router's DHCP server.

Note: Please make sure that the router's DHCP server is the only DHCP server available on your LAN. Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

2b) Windows 2000

i: Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.

ii: Double-click the *Network and Dial-up Connections* icon. In the *Network and Dial-up Connection* window, double-click the *Local Area Connection* icon. The *Local Area Connection* window will appear.

iii: In the *Local Area Connection* window, click the *Properties* button.

iv: Check your list of Network Components. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.

v: In the Internet Protocol (TCP/IP) Properties window, select *Obtain an IP address automatically* and *Obtain DNS server address automatically* as shown on the following screen.
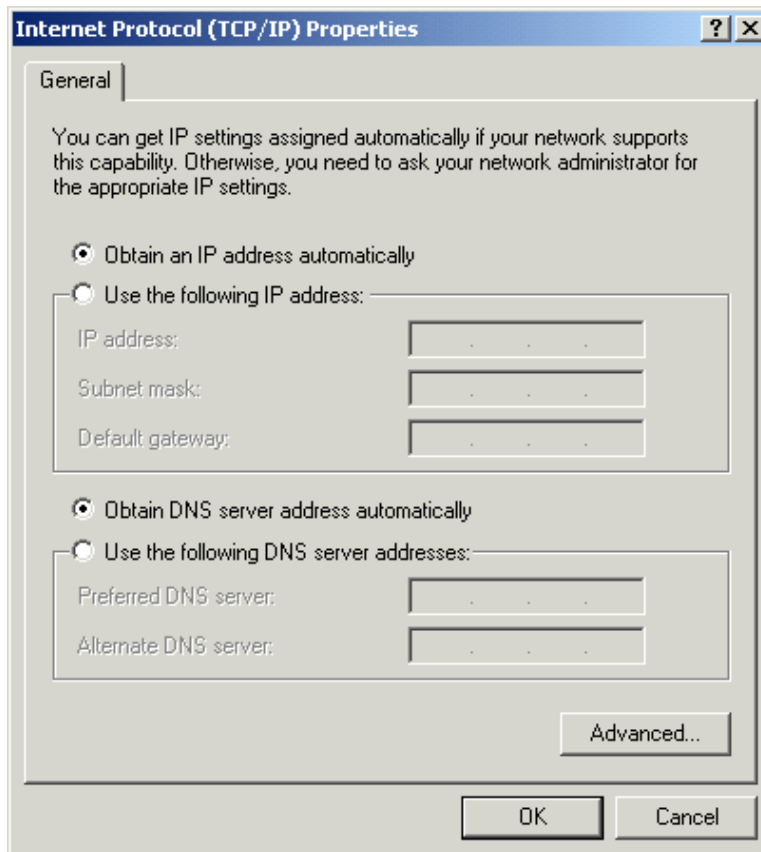
Figure 0.4

vi: Click *OK* to confirm the settings. Your PC will now obtain an IP address automatically from your router's DHCP server.

Note: Please make sure that the router's DHCP server is the only DHCP server available on your LAN. Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

2c) Windows NT

i: Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.

ii: Double-click the *Network* icon. The *Network* window will appear. Select the *Protocol* tab from the *Network* window.

iii: Check if the *TCP/IP Protocol* is on your list of *Network Protocols*. If TCP/IP is not installed, click the *Add* button to install it now. If TCP/IP is installed, go to step 5.

iv: In the *Select Network Protocol* window, select the *TCP/IP Protocol* and click the *Ok* button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.

v: After you install TCP/IP, go back to the *Network* window. Select *TCP/IP* from the list of *Network Protocols* and then click the *Properties* button.

vi: Check each of the tabs and verify the following settings:

- **IP Address:** Select *Obtain an IP address from a DHCP server*.
- **DNS:** all fields are blank.
- **WINS:** all fields are blank.
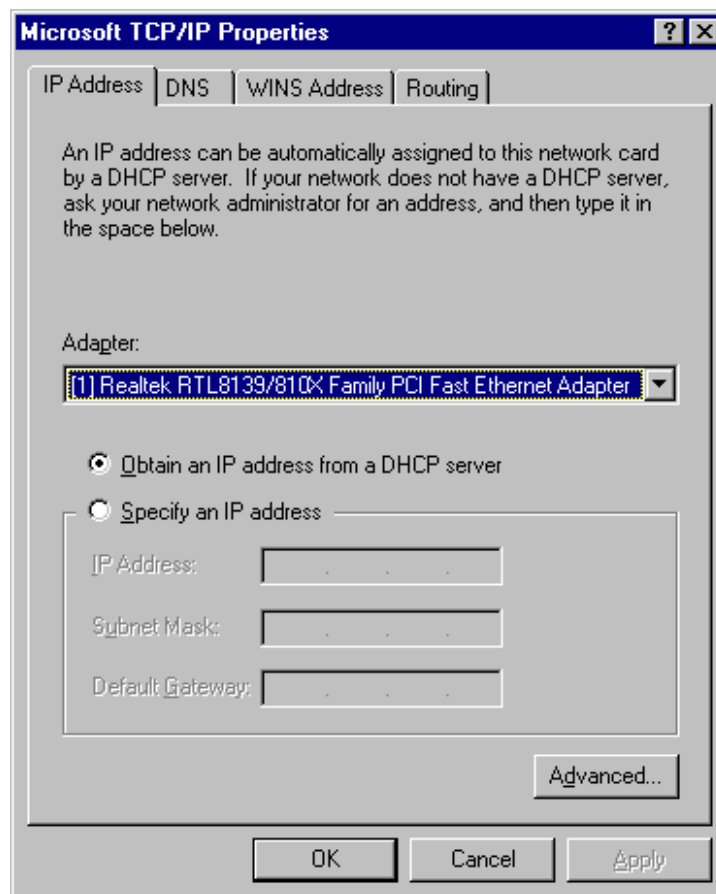- **Routing:** all fields are blank.

Figure 0.4

vii: Click *OK* to confirm the settings. Your PC will now obtain an IP address automatically from your router's DHCP server.

Note: Please make sure that the router's DHCP server is the only DHCP server available on your LAN. Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

3) Once you have configured your PCs to obtain an IP address automatically, the router's DHCP server will automatically give your LAN clients IP addresses. By default, the router's DHCP server is enabled so that you can obtain an IP address automatically. To see if you have obtained an IP address, see Appendix A.

Note: Please make sure that the router's DHCP server is the only DHCP server available on your LAN. If there is another DHCP server on your network, then you'll need to switch one of the DHCP servers off. (To disable the router's DHCP server, see Chapter 2: LAN Port.)

4) Once your *PC* has obtained an IP address from your router, enter the *router's* default IP address of "**192.168.2.1"** into your PC's web browser and press *Enter*.
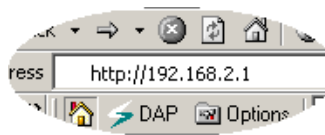

Figure 0.5

5) The login screen below will appear. Enter the "User Name" and "Password" and then click <OK> to login.

Note: By default the user name is "admin" and the password is "1234". For security reasons it is recommended that you change the password as soon as possible (in General setup/system/password, see chapter 2)
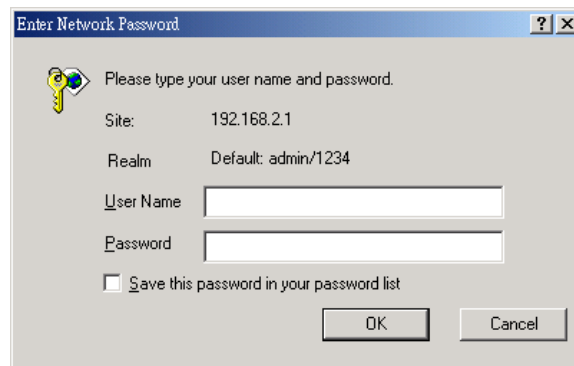

Figure 0.6

6)   The HOME page screen below will appear. The Home Page is divided into four sections, Quick Setup Wizard, General Setup, Status Information and Tools.

Quick Setup Wizard *(Chapter 1)*
If you only want to start using the router as an Internet Access device then you ONLY need to   configure the screens in the Quick Setup Wizard section.

General Setup *(Chapter 2)*
If you want to use more advanced features that the router has to offer, then you will need to configure the Quick Setup Wizard and the General Setup section. Alternatively, you can just configure the General Setup section, since the General Setup/WAN and the Quick Setup Wizard contain the same configurations.

Status Information *(Chapter 3)*
The Status Information section is for you to monitor the router's status information at any point in time.

Tools *(Chapter 4)*
If you want to Reset the router (because of problems) or save your configurations or upgrade the firmware then you will need to go to the Tools section.
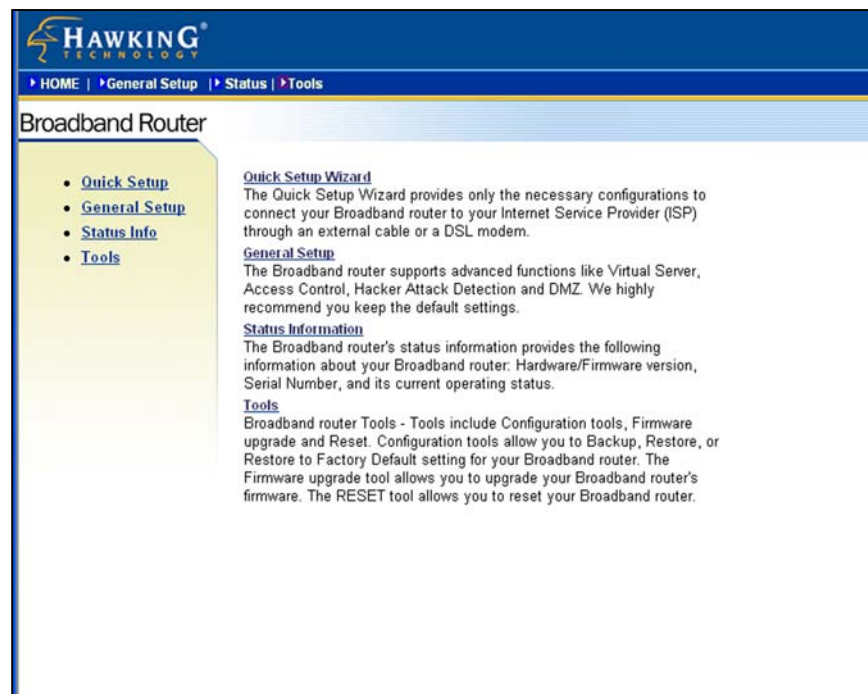

Figure 0.7

Introduction

H2BR4 Dual WAN 4-Port Firewall Router

Menu	Description
Quick Setup Wizard *(Chapter 1)*	Select your Internet connection type and then input the configurations needed to connect to your Internet Service Provider (ISP).
General Setup *(Chapter 2)*	This section contains configurations for the Broadband router's advanced functions such as: Bridge, Address Mapping, Virtual Server, Access Control, Hacker Attack Prevention, DMZ, Special applications and other functions to meet your LAN requirements.
Status Information *(Chapter 3)*	In this section you can see the Broadband router's system information, Internet Connection, Device Status, Security Log and DHCP client Log information.
Tools *(Chapter 4)*	This section contains the router's Tools - Tools include Configuration tools, Firmware upgrade and Reset. Configuration tools allow you to Backup (save), Restore, or Restore to Factory Default configuration for your Broadband router. The Firmware upgrade tool allows you to upgrade your router's firmware. The RESET tool allows you to reset your Broadband router.
Logout	Selecting logout will return you to the LOGIN page

7) Click on Quick Setup Wizard (see Chapter 1) to start configuring settings required by your ISP so that you can start accessing the Internet. The other sections (General Setup, Status Information and Tools) do not need to be configured unless you wish to implement/monitor more advanced features/information.

Select the section (Quick Setup Wizard, General Setup, Status Information and Tools) you wish to configure and proceed to the corresponding chapter. Use the selections on the web management's top right hand page (see below) to navigate around the web-based management User Interface.
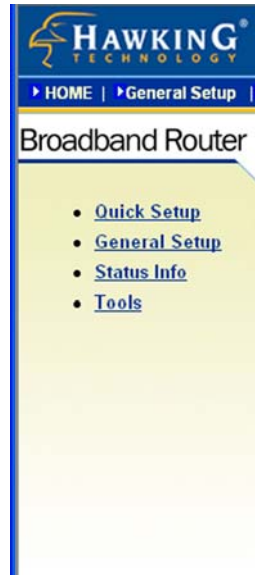
Figure 0.8

About Quick Setup

The Quick Setup section is designed to let you set up the router as quickly as possible. In the Quick Setup, you are required to fill in only the information necessary to access the Internet. Once you click on the **Quick Setup Wizard** in the homepage, you will see the screen below.

Step 1) Time Zone

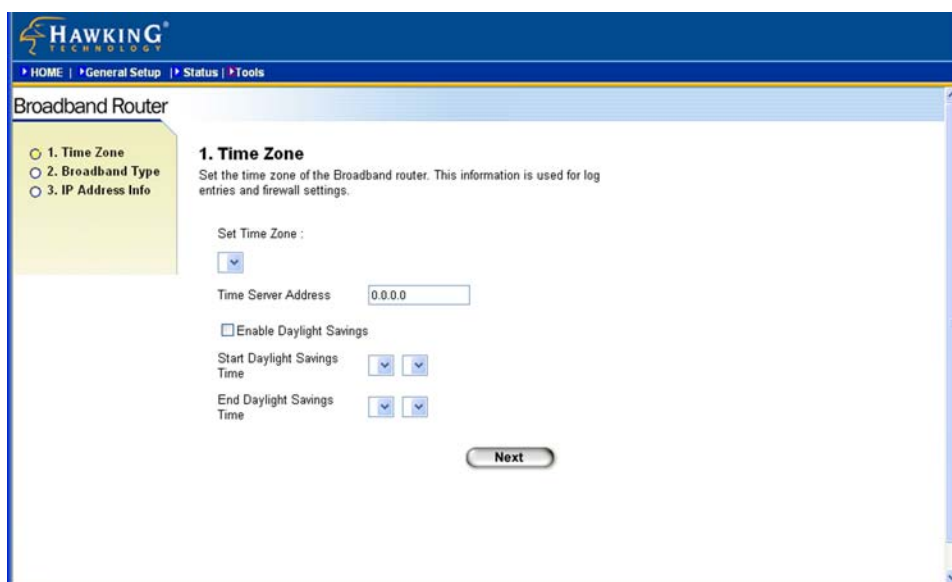The Time Zone allows your router to base its time on the settings configured here, this will affect functions such as Log entries and Firewall settings.

Figure 1.1

Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Time Server Address	You can manually assign the time server address if the default time server does not work.
Enable Daylight Savings	The router can also take Daylight savings into account. If you wish to use this function, you must check the "Enable Daylight Savings" box to enable your daylight savings configuration (below).
Start Daylight Savings Time	Select the period in which you wish to start daylight Savings Time
End Daylight Savings Time	Select the period in which you wish to end daylight Savings Time

Click on **NEXT** to proceed to the next page (step 2).

Step 2) Broadband Type

In this section, you have to select one of four types of connections that you will be using to connect your router's WAN port to your ISP (see screen below).

Note: Different ISP's require different methods of connecting to the Internet. Please check with your ISP as to the type of connection it requires.
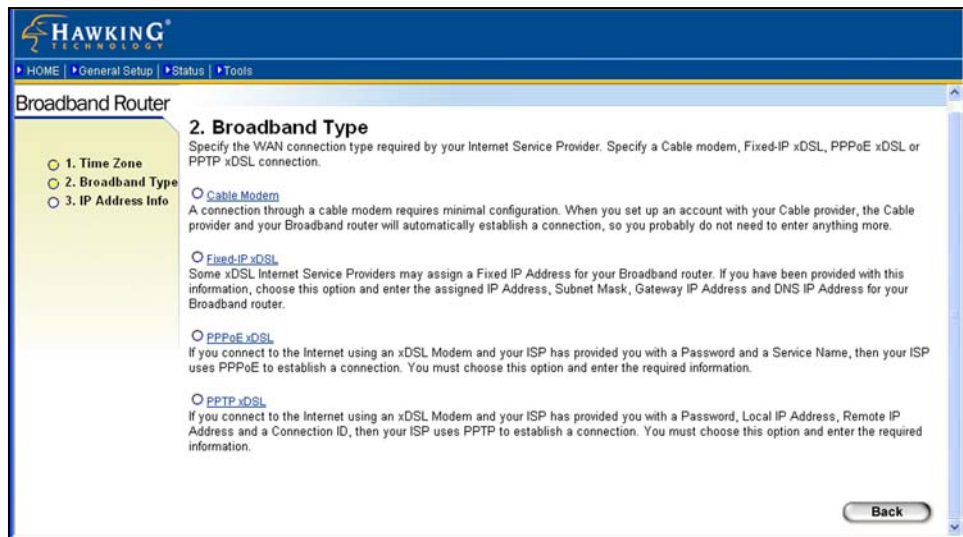

Figure 1.2

Menu	Description
1.1 Cable Modem	Your ISP will automatically give you an IP address
1.2 Fixed-IP xDSL	Your ISP has given you an IP address already
1.3 PPPoE	Your ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection.
1.4 PPTP	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.

Click on one of the WAN types and then proceed to the manual's relevant sub-section (**1.1**, **1.2**, **1.3** or **1.4**). Click on **Back** to return to the previous screen.

1.1 Cable Modem
Choose Cable Modem if your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as Host Name and MAC address (see screen below).

Note: The Host Name and MAC address section is *optional* and you can skip this section if your ISP does not require these settings for you to connect to the Internet.

Figure 1.3

Parameters	Description
Host Name	If your ISP requires a Host Name, type in the host name provided by your ISP; otherwise leave it blank if your ISP does not require a Host Name.
MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. *__This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to__*. Type in this MAC address in this section or use the "**Clone MAC Address"** button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work). To find out the PC's MAC address see Appendix A. (See Glossary for an explanation on MAC addresses.)

Click **OK** when you have finished the configuration above. You have now completed the configuration for the Cable Modem connection. You can start using the router now. If you wish to use some of the advanced features supported by this router, see Chapters 2, 3, 4.

1.2 Fixed-IP xDSL

Select "Fixed-IP xDSL" if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section.

Figure 1.4

Parameters	Description
IP	This is the IP address that your ISP has given you.
Gateway IP	This is the ISP's IP address gateway
DNS	This is the ISP's DNS server IP address
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)

Click **OK** when you have finished the configuration above. You have now completed the configuration for the Fixed-IP xDSL connection. You can start using the router now. If you wish to use some of the advanced features supported by this router, see Chapters 2, 3, 4.

1.3 PPPoE

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

Figure 1.5

Quick Setup

H2BR4 Dual WAN 4-Port Firewall Router

Parameter	Description
User Name	Enter the User Name provided by your ISP for the PPPoE connection
Password	Enter the Password provided by your ISP for the PPPoE connection
Service Name	This is optional. Enter the Service name should your ISP require it. Otherwise, leave it blank.
MTU	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size.
Connection Type	If you select "Continuous", the router will always be connected to the ISP/Internet. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP. If you select "Connect On Demand", the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period during which no one has been using the Internet exceeds the "Idle Time". If you select "Manual", the router will connect to the ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not get disconnected due to the idle timeout. If the WAN line breaks down and later links again, the router will not auto-connect to the ISP.
Idle Time	You can specify an idle time threshold (in minutes) for the WAN port. This means if no packets have been sent (no one is using the Internet) during this specified period, the router will automatically disconnect the connection to the ISP/Internet. **Note:** The WAN "idle timeout" auto-disconnect function may not work due to abnormal activities of some network application software, computer viruses or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. This function also may not work with some ISPs. Please make sure this function can work properly when you use this function the first time, especially if your ISP charges you by time used. Due to various uncontrollable issues, we cannot guarantee the WAN "idle timeout" auto-disconnect function will always work. In order to prevent an extra fee from being charged by your ISP, please *turn off the router when you are finished using the Internet.*

Click **OK** when you have finished the configuration above. You have now completed the configuration for the PPPoE connection. You can start using the router now. If you wish to use some of the advanced features supported by this router, see Chapters 2, 3, 4.

1.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

Figure 1.6

Parameter	Description
Obtain an IP address	The ISP requires you to obtain an IP address by DHCP automatically before connecting to the PPTP server.
Use the following IP address	The ISP gives you a static IP to be used to connect to the PPTP server.
IP Address	This is the IP address that your ISP has given you to establish a PPTP connection.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Default Gateway	Enter the IP address of the ISP Gateway

User ID	Enter the User Name provided by your ISP for the PPTP connection (sometimes called a Connection ID).
Password	Enter the Password provided by your ISP for the PPTP connection.
PPTP Gateway	If your LAN has a PPTP gateway, then enter that PPTP gateway IP address here. If you do not have a PPTP gateway then enter the ISP's Gateway IP address above.
Connection ID	This is the ID given by ISP. This is optional.
MTU	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size.
BEZEQ-ISRAEL	Select this item if you are using the service provided by BEZEQ in Israel.
Connection Type	If you select "Continuous", the router will always be connected to the ISP/Internet. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP. If you select "Connect On Demand", the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period during which no one has been using the Internet exceeds the "Idle Time". If you select "Manual", the router will connect to the ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not get disconnected due to the idle timeout. If the WAN line breaks down and later links again, the router will not auto-connect to the ISP.
Idle Time	You can specify an idle time threshold (in minutes) for the WAN port. This means if no packets have been sent (no one is using the Internet) during this specified period, the router will automatically disconnect the connection to the ISP/Internet. **Note:** The WAN "idle timeout" auto-disconnect function may not work due to abnormal activities of some network application software, computer viruses or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. This function also may not work with some ISPs. Please make sure this function can work properly when you use this function the first time, especially if your ISP charges you by time used. Due to various uncontrollable issues, we cannot guarantee the WAN "idle timeout" auto-disconnect function will always work. In order to prevent an extra fee from being charged by your ISP, please *turn off the router when you are finished using the Internet.*

Click **OK** when you have finished the configuration above. You have now completed the configuration for the PPTP connection. You can start using the router now. If you wish to use some of the advanced features supported by this router, see Chapters 2, 3, 4.

General Settings

Once you click on the **General Setup** button on the homepage, you will see the screen below.

If you have already configured the Quick Setup Wizard, you do NOT need to configure anything in the General Setup screen in order to start using the Internet.

The General Setup contains advanced features that allow you to configure the router to meet your network's needs such as: Address Mapping, Virtual Server, Access Control, Hacker Attack Prevention, Special Applications, DMZ and other functions.
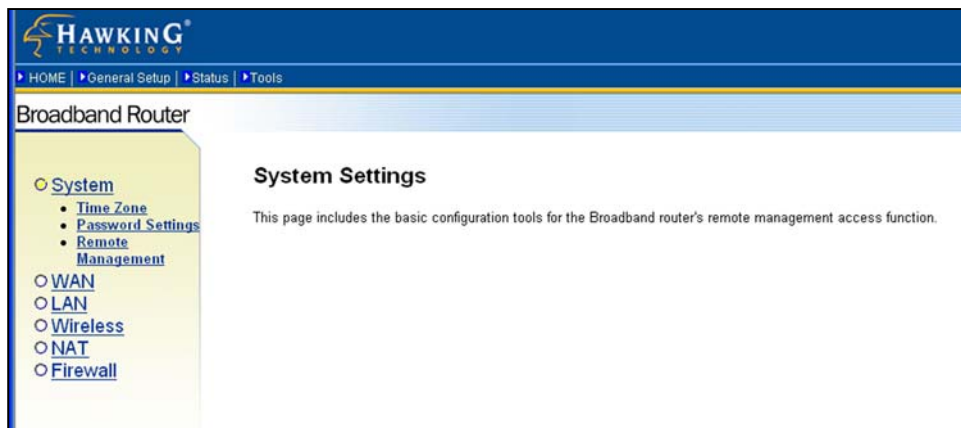

Figure 2.1

General Setup
H2BR4 Dual WAN 4-Port Firewall Router

Below is a general description of what advanced functions are available for this broadband router.

Menu	Description
2.1 System	This section allows you to set the Broadband router's system Time Zone, Password and Remote Management Administrator.
2.2 WAN	This section allows you to select the connection method in order to establish a connection with your ISP (same as the Quick Setup Wizard section)
2.3 LAN	You can specify the LAN segment's IP address, subnet Mask, enable/disable DHCP and select an IP range for your LAN
2.4 NAT	You can configure the Address Mapping, Virtual Server and Special Applications functions in this section. This allows you to specify what user/packet can pass your router's NAT.
2.5 Firewall	The Firewall section allows you to configure Access Control, Hacker Prevention and DMZ.

Select one of the General Setup selections from above and proceed to the manual's relevant sub-sections.

2.1 System

The system screen allows you to specify a time zone, to change the system password and to specify a remote management user for the broadband router.
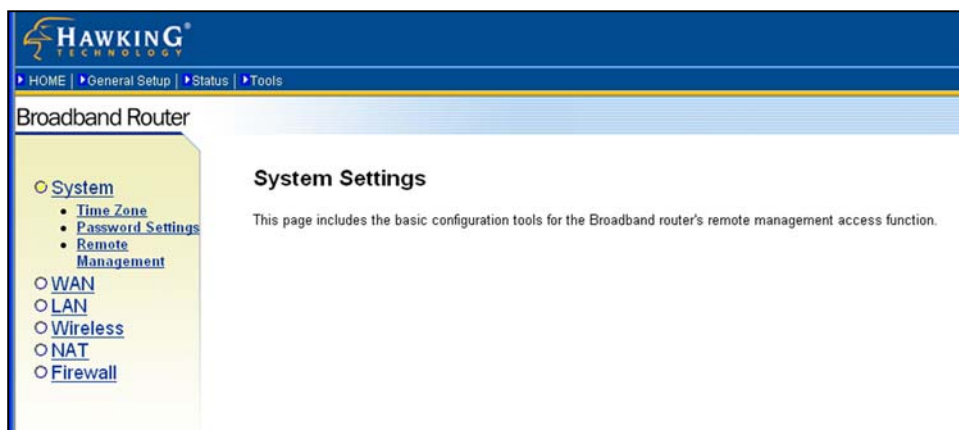

Figure 2.2

Parameters	Description
System Settings	
2.1.1 Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
2.1.2 Password Settings	Allows you to select a password in order to access the web-based management website.
2.1.3 Remote Management	You can specify a Host IP address that can perform remote management functions.

Select one of the above three system settings selections and proceed to the manual's relevant sub-sections.

2.1.1 Time Zone
The Time Zone allows your router to reference or base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.
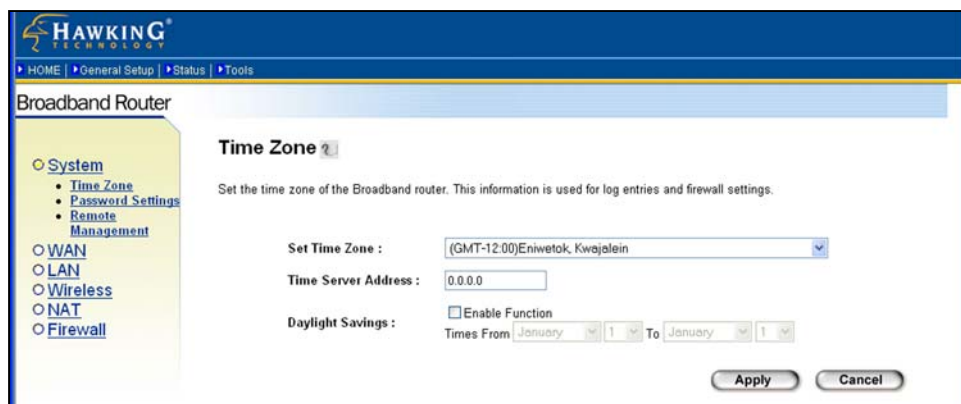

Figure 2.3

General Setup

H2BR4 Dual WAN 4-Port Firewall Router

Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Time Server Address	You can manually assign time server address if the default time server dose not work.
Enable Daylight Savings	The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below).
Start Daylight Savings Time	Select the period in which you wish to start daylight Savings Time
End Daylight Savings Time	Select the period in which you wish to end daylight Savings Time

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

2.1.2 Password Settings

You can change the password required to log into the broadband router's system web-based management. By default, the password is "1234". So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.
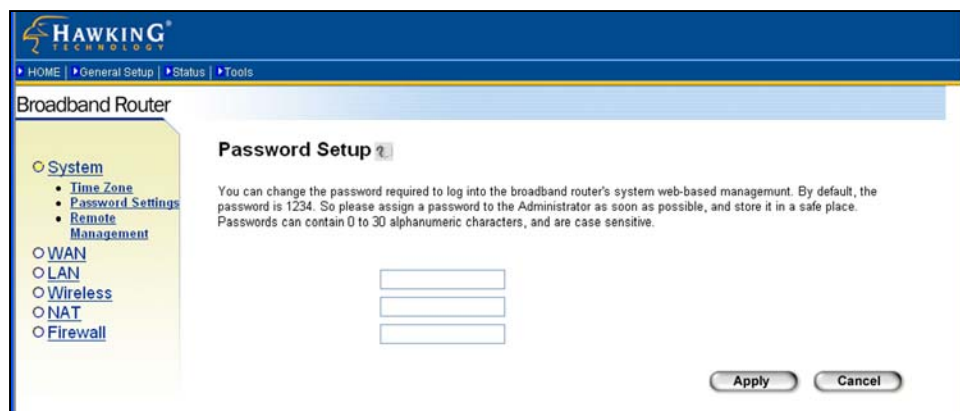

Figure 2.4

Parameters	Description
Current Password	Enter your current password for the remote management administrator to log in to your router. Note: By default, the password is "**1234**"
New Password	Enter your new password
Re-Enter Password for Verification	Enter your new password again for verification purposes **Note**: If you forget your password, you will have to reset the router to the factory default (password is "1234") with the reset button (see router's back panel).

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

2.1.3 Remote Management
The remote management function allows you to provide a host on the Internet with the ability to configure the router from a remote site. Enter the designated host IP Address in the Host IP Address field.
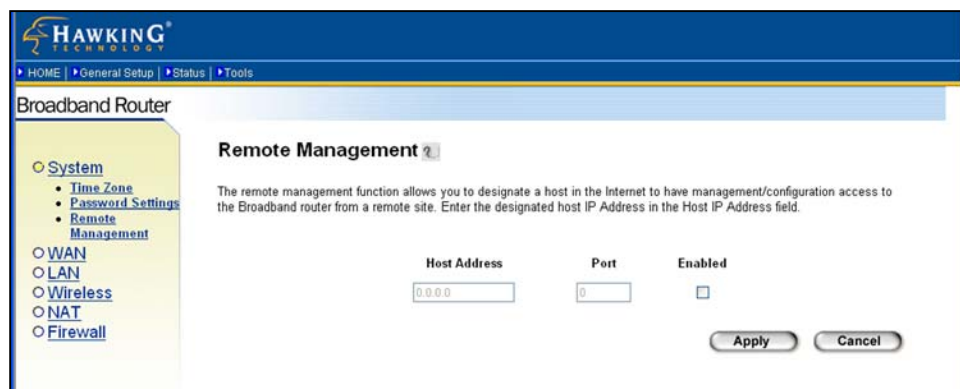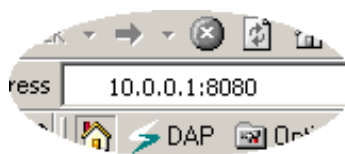

Figure 2.5

General Setup

H2BR4 Dual WAN 4-Port Firewall Router

Parameters	Description
Host Address	This is the IP address of the host on the Internet that will have management/configuration access to the Broadband router from a remote site. This means if you are at home and your home IP address has been designated the Remote Management host IP address for this router (located in your company office), then you are able to configure this router from your home. If the Host Address is left **0.0.0.0** this means anyone can access the router's web-based configuration from a remote location, provided that they know the password. Click the **Enabled** box to enable the Remote Management function. **Note**: When you want to access the web-based management from a remote site, you must enter the router's WAN IP address (e.g. 10.0.0.1) into your web-browser followed by port number 8080, e.g. 10.0.0.1:8080 (see below). You'll also need to know the password set in the Password Setting screen in order to access the router's web-based management.

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

2.2 WAN

Use the **WAN Settings** screen if you have already configured the router via the Quick Setup Wizard section and you would like to change your Internet connection type. The **WAN Settings** screen allows you to specify the type of WAN port connection you want to establish with your ISP. In the **WAN Settings** screen, you can also configure the router to act as a bridge. The WAN settings offer the following selections for the router's WAN port: **Dynamic IP**, **Static IP**, **PPPoE**, **PPTP**, **L2TP**, **Telstra Big Pond**, **Policy**, **DNS** and **DDNS**. You will need to select one of the two WAN ports first and configure one WAN port at a time.

General Setup

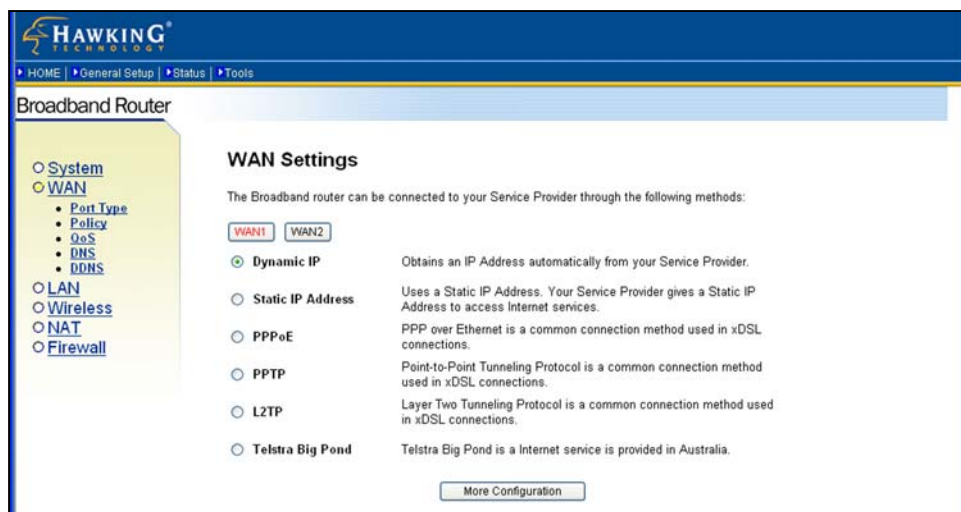H2BR4 Dual WAN 4-Port Firewall Router

Figure 2.6

Parameters	Description
2.2.1 Dynamic IP address	Your ISP will automatically give you an IP address
2.2.2 Static IP address	Your ISP has given you an IP address already
2.2.3 PPPoE	Your ISP requires PPPoE connection.
2.2.4 PPTP	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
2.2.5 L2TP	Your ISP requires L2TP connection.
2.2.6 Telstra Big Pond	Your ISP requires Telstra Big Pond connection.
2.2.7 Policy	You can configure WAN policy.
2.2.8 DNS	You can specify a DNS server that you wish to use
2.2.9 DDNS	You can specify a DDNS server that you wish to use and configure the user name and password provided by your DDNS service provider.

Once you have made a selection, click **More Configuration** at the bottom of the screen and proceed to the manual's relevant sub-sections.

2.2.1 Dynamic IP Address

Choose the Dynamic IP selection if your ISP will give you an IP address automatically. Some ISP's may also require that you fill in additional information such as Host Name, Domain Name and MAC address. (See Chapter 1: "Cable Modem" for more details.)

2.2.2 Static IP Address

Choose the Static IP selection if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section. (See Chapter 1: "Fixed IP" for more details.)

2.2.3 PPPoE (PPP over Ethernet)

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section. (See chapter 1 "PPPoE" for more details.)

2.2.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section. (See chapter 1: "PPTP" for more details.)

2.2.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

Figure 2.7

General Setup

H2BR4 Dual WAN 4-Port Firewall Router

Parameter	Description
Obtain an IP address	The ISP requires you to obtain an IP address by DHCP automatically before connecting to the L2TP server.
MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the "Clone MAC Address" button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work). To find out the PC's MAC address see Appendix A. (see Glossary for an explanation on MAC address)
Use the following IP address	The ISP gives you a static IP address to be used to connect to the L2TP server.
IP Address	This is the IP address that your ISP has given you to establish an L2TP connection.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP Gateway
User ID	Enter the User Name provided by your ISP for the PPTP connection. Sometimes called a Connection ID
Password	Enter the Password provided by your ISP for the PPTP connection
L2TP Gateway	If your LAN has an L2TP gateway, then enter that L2TP gateway IP address here. If you do not have an L2TP gateway, then enter the ISP's Gateway IP address above.
MTU	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size.
Connection Type	If you select "Continuous", the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP. If you select "Connect On Demand", the router will auto-connect to the ISP when someone want to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time". If you select "Manual", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP.

Idle Time Out

Note: The WAN "idle timeout" auto-disconnect function may not work due to abnormal activities of some network application software, computer viruses or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. This function also may not work with some ISPs. Please make sure this function can work properly when you use this function the first time, especially if your ISP charges you by time used. Due to various uncontrollable issues, we cannot guarantee the WAN "idle timeout" auto-disconnect function will always work. In order to prevent an extra fee from being charged by your ISP, please *turn off the router when you are finished using the Internet.*

Click **OK** when you have finished the configuration above. You have now completed the configuration for the L2TP connection. You can start using the router now. If you wish to use some of the advanced features supported by this router, see Chapters 2, 3, 4.

2.2.6 Telstra Big Pond

Select Telstra Big Pond if your ISP requires the Telstra Big Pond protocol to connect you to the Internet. Your ISP should provide all the information required in this section. Telstra Big Pond protocol is used by ISPs in Australia.

Figure 2.8

Parameter	Description
User Name	Enter the User Name provided by your ISP for the Telstra Big Pond connection
Password	Enter the Password provided by your ISP for the Telstra Big Pond connection
User decide login server server manually	Select if you want to assign the IP of Telstra Big Pond's login server manually.
Login Server	The IP of the Login Server.

Click **OK** when you have finished the configuration above. You have now completed the configuration for the Telstra Big Pond connection. You can start using the router now. If you wish to use some of the advanced features supported by this router, see Chapters 2, 3, 4.

2.2.7 WAN Policy

The WAN policy for multi-homing can be setup here. You can set up policy for each WAN separately. The router will balance the load between all active WAN ports according to the Send/Receive rate of the WAN ports. You can setup an IP address for the router to detect if the WAN line is connected. If the router fails to ping the IP, it would recognize the WAN line as not connected, and will stop directing the Internet traffic to this WAN port. The traffic will be redirected to the other active WAN port. The Intranet users will not become aware of this change and keep surfing the Internet smoothly. You also can setup a WAN port as a backup WAN port. A backup WAN port would not be activated when the router starts up. When the other active WAN port fails to connect to the Internet, the backup WAN port will be activated and take over all the traffic.

Figure 2.9

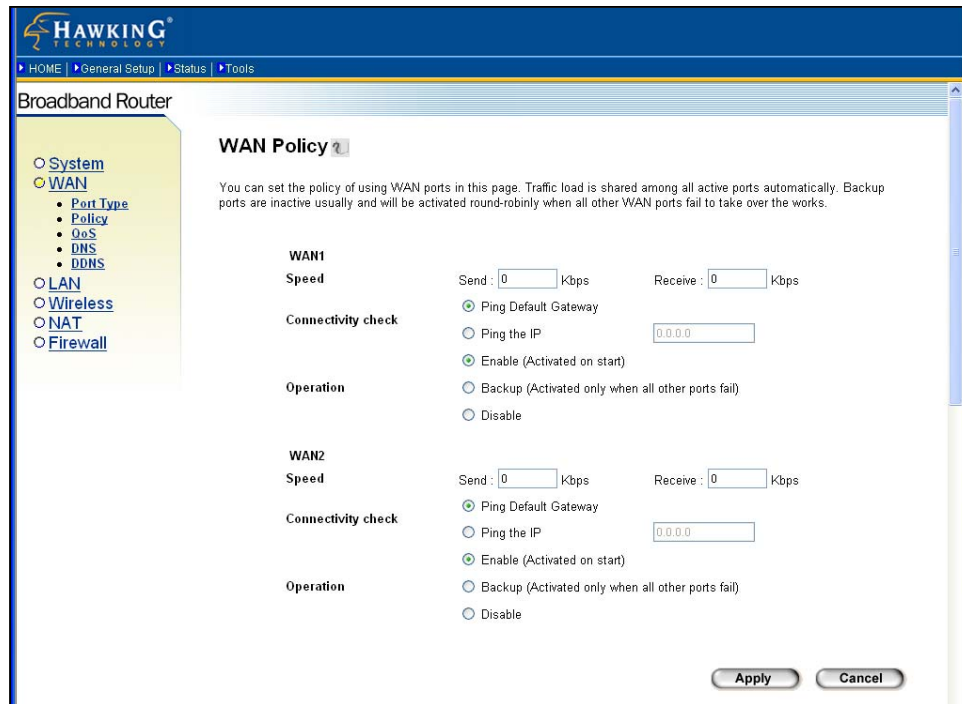| Parameter	Description
Speed	The send/upstream and receive/downstream speed of the WAN line the WAN port is connected to.
Connectivity check	You can key in an IP. The router will ping that IP to verify if the WAN line can access the Internet. You also can select "Ping Default Gateway", and the router will check if the WAN line is ok by ping the default gateway of the WAN port.
Operation	If you select "Enable", the WAN port will be activated when the system boot up. If you select "Backup", the WAN port is disabled on start up. But when other enabled WAN ports fail, the backup WAN port will be activated and take over all the traffic.

2.2.8 DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.router.com, a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for speed and convenience. If your Service Provider connects you to the Internet with

dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that you would rather use, you need to specify the IP address of that DNS server here.
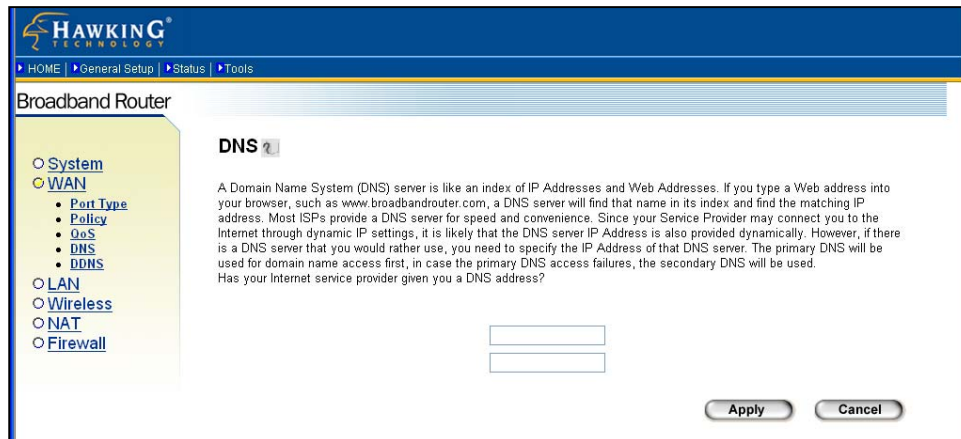
Figure 2.10

Parameters	Description
Domain Name Server (DNS) Server	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address
Secondary DNS Address (optional)	This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used should the above DNS fail.

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

2.2.9 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. You can assign a DDNS server for each WAN port. This router supports some DDNS service providers, for example DynDNS and TZO.
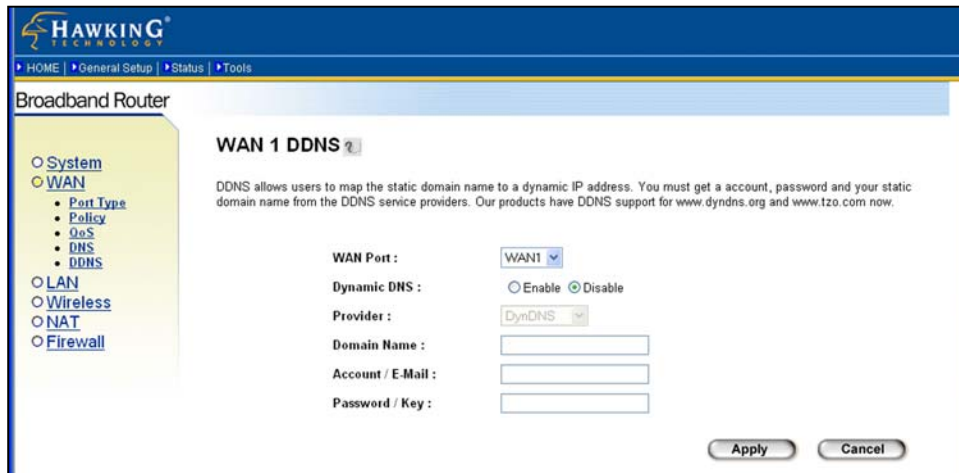
Figure 2.11

Parameters	Default	Description
WAN Port		Select the WAN port that you want to configure the DDNS for
Enable/Disable	Disable	Enable/Disable the DDNS function of this router
Provider	DynDNS	Select a DDNS service provider
Domain name		Your static domain name that use DDNS
Account/E-mail		The account that your DDNS service provider assigned to you
Password/Key		The password you set for the DDNS service account above

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

2.3 LAN

The LAN Port screen below allows you to specify a private IP address for your router's LAN ports as well as a subnet mask for your LAN segment.

Figure 2.12

General Setup

H2BR4 Dual WAN 4-Port Firewall Router

Parameters	Default	Description
LAN		
IP address	192.168.2.1	This is the router's LAN port (private) IP address (Your LAN clients' default gateway IP address)
IP Subnet Mask	255.255.255.0	Specifies a Subnet Mask for your LAN segment
802.1d Spanning Tree	Disabled	If the 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops from occurring among the LAN ports.
DHCP Server	Enabled	You can enable or disable the DHCP server. By enabling the DHCP server, the router will automatically give your LAN clients an IP address. If the DHCP is not enabled then you'll have to manually set your LAN clients' IP addresses; make sure the LAN Client is in the same subnet as the router if you want the router to be your LAN clients' default gateway
Lease Time		When DHCP is enabled, it will temporarily give your LAN clients an IP address. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time threshold period is reached
IP Address Pool		You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. **Note:** By default the IP range is from: Start IP **192.168.2.100** to End IP **192.168.2.199**. If you want your PC to have a static/fixed IP address then you'll have to choose an IP address outside this IP address Pool
Domain Name		You can specify a Domain Name for your LAN

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

General Setup

H2BR4 Dual WAN 4-Port Firewall Router

2.4 NAT

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. You also can disable NAT function and use the static route.
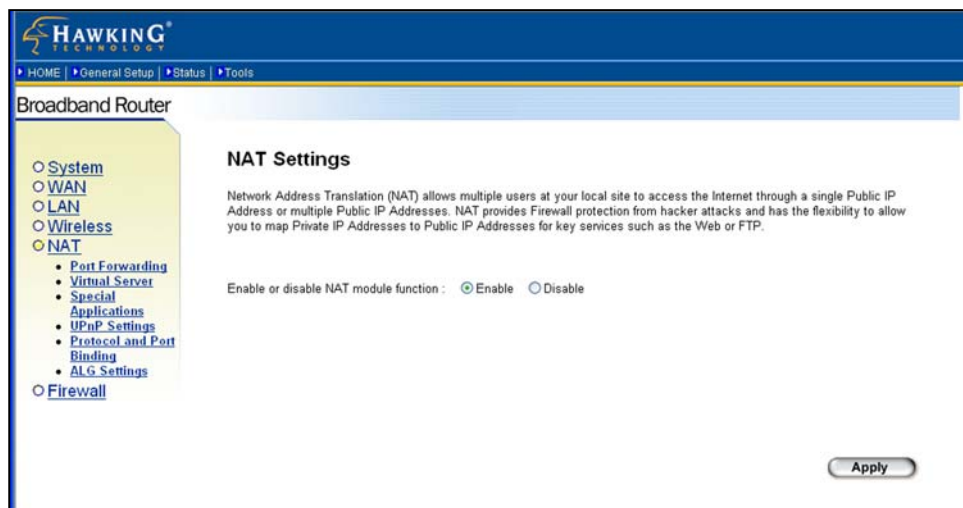
Figure 2.13

Parameter	Description
Enable or Disable NAT	You can enable NAT to let the router provide the IP sharing function or disable NAT to use the static routing function.

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

2.4.1 Port Forwarding

The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the router NAT firewall.

Figure 2.14

Parameter	Description
Enable Port Forwarding	Enable Port Forwarding
Private IP	This is the private IP of the server behind the NAT firewall. **Note:** You need to give your LAN PC clients a fixed/static IP address for Port Forwarding to work properly.
Type	This is the protocol type to be forwarded. You can choose to forward "TCP" or "UDP" packets only or select "both" to forward both "TCP" and "UDP" packets.
Port Range	The range of ports to be forward to the private IP.
WAN Port	Assign the WAN port that requires port forwarding. All the packets sent from this WAN port with the assigned port range will be directed to the assigned private IP addresses.
Comment	The description of this setting.
Add Port Forwarding into the table	Fill in the "Private IP", "Type", "Port Range", "WAN Port" and "Comment" of the settings to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below. If you find any errors before adding it and want to type it in again, just click "Clear" and the fields will be cleared.
Remove Port Forwarding into the table	If you want to remove some Port Forwarding settings from the " Current Port Forwarding Table", select the Port Forwarding settings you want to remove in the table and then click "Delete Selected". If you want to remove all Port Forwarding settings from the table, just click the "Delete All" button. Clicking "Reset" will clear your current selections.

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

2.4.2 Virtual Server

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number. (See Glossary for an explanation on Port number)
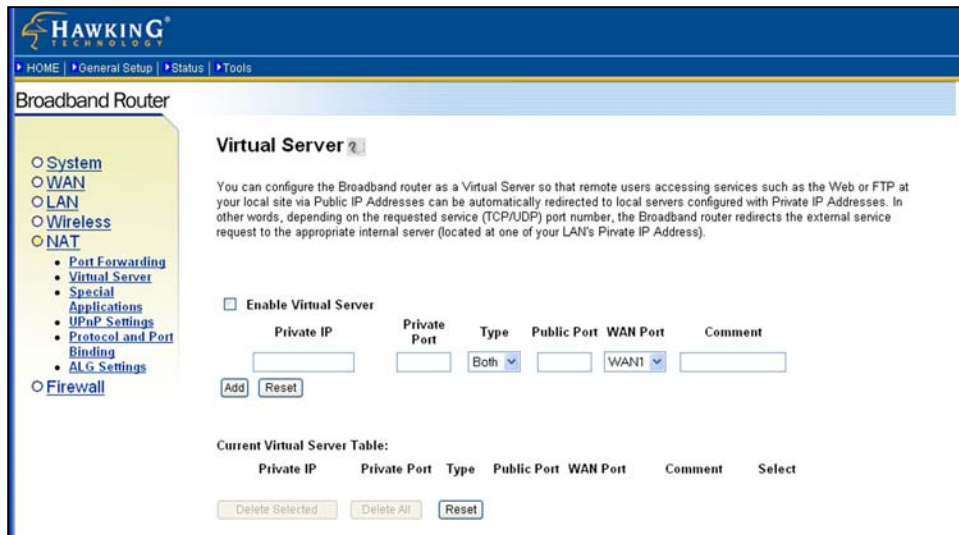

Figure 2.15

General Setup

H2BR4 Dual WAN 4-Port Firewall Router

Parameters	Description
Enable Virtual Server	Enable Virtual Server.
Private IP	This is the LAN client/host IP address that the Public Port number packet will be sent to. **Note:** You need to give your LAN PC clients a fixed/static IP address for the Virtual Server function to work properly.
Private Port	This is the port number (of the above Private IP host) that the below Public Port number will be changed to when the packet enters your LAN (to the LAN Server/Client IP)
Type	Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default "Both" protocol.
Public Port	Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN **Note**: Virtual Server function will have priority over the DMZ function if there is a conflict between the Virtual Server and the DMZ settings.
WAN Port	Assign the WAN port that you want to bind to the virtual server. All the packets sending from this WAN port with the assigned public port will be directed to the assigned private IP and private port.
Comment	The description of this setting.
Add Virtual Server	Fill in the "Private IP", "Private Port", "Type", "Public Port", "WAN Port" and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below. If you find any errors before adding it and want to retype again, just click "Clear" and the fields will be cleared.
Remove Virtual Server	If you want to remove some Virtual Server settings from the "Current Virtual Server Table", select the Virtual Server settings you want to remove in the table and then click "Delete Selected". If you want remove all Virtual Server settings from the table, just click the "Delete All" button. Clicking "Reset" will clear your current selections.

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

Example: Virtual Server

The diagram below demonstrates one of the ways you can use the Virtual Server function. Use Virtual Server when you want the web server located in your private LAN to be accessible to Internet users from WAN 2. The configuration below means that any request coming form the Internet to access your web server will be translated to your LAN's web server (192.168.2.2). **Note:** For the virtual server to work properly Internet/remote users must know your global IP

address for WAN 2. (For websites, you will need to have a fixed/static global/public IP address or use DDNS with dynamic IP and domain name mapping.)
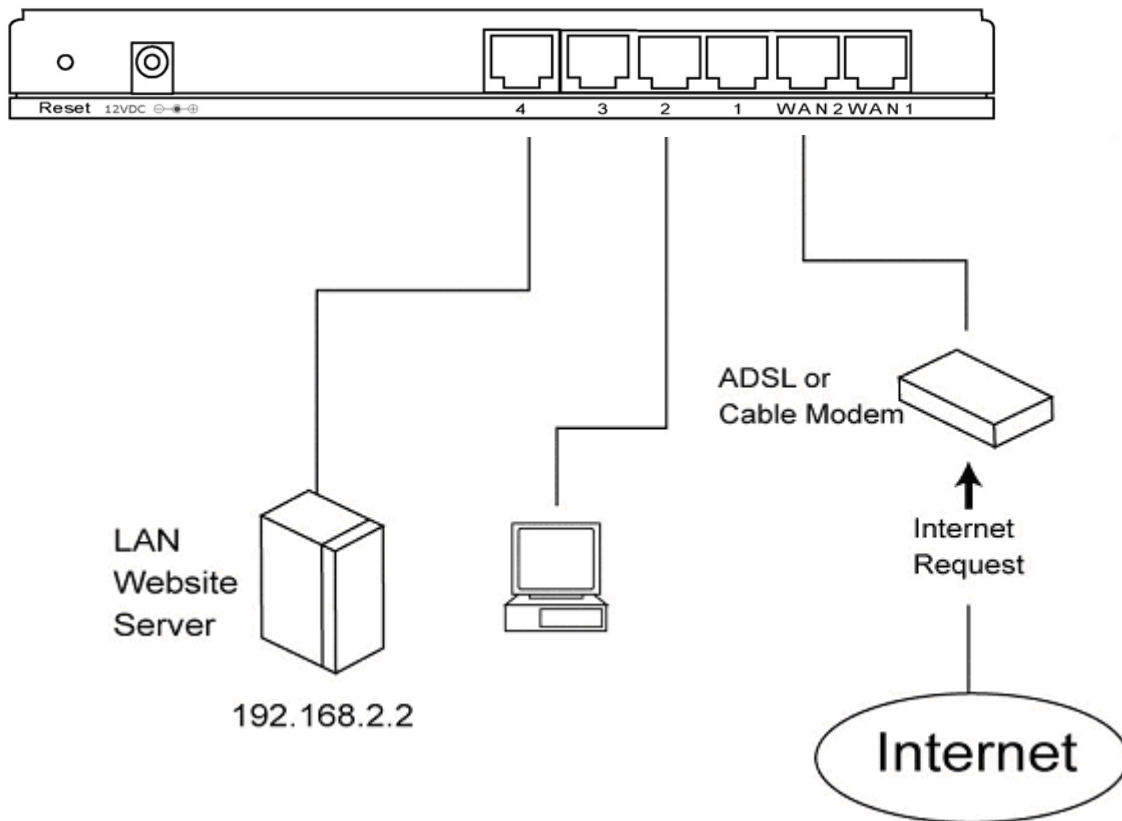
Figure 2.16

2.4.3 Special Applications

Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.
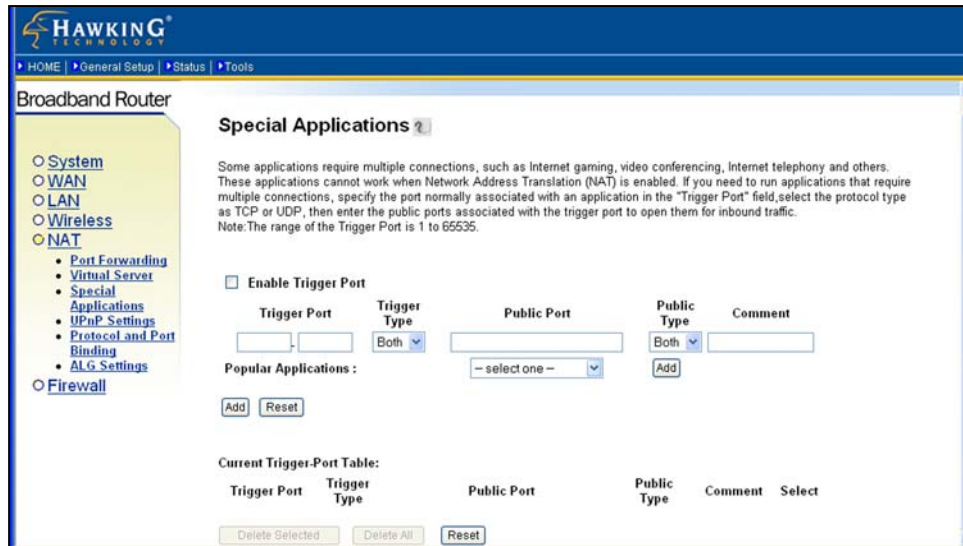
Figure 2.17

Parameters	Description
Enable Trigger Port	Enables the Special Application function.
Trigger Port	This is the outgoing (Outbound) range of port numbers for this particular application
Trigger Type	Select whether the outbound port protocol is "TCP", "UDP" or both.
Public Port	Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624) **Note**: Individual port numbers are separated by a comma (e.g. 47624, 5775, 6541 etc.). To input a port range use a "dash" to separate the two port number range (e.g. 2300-2400)
Public Type	Select the Inbound port protocol type: "TCP", "UDP" or both
Comment	The description of this setting.

Popular applications	This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, select a location (1-10) in the **Copy to** selection box and then click the **Copy to** button. This will automatically list the Public Ports required for this popular application in the location (1-10) you had specified.
Add Special Application	Fill in the "Trigger Port", "Trigger Type", "Public Port", "Public Type", and "Comment" of the setting to be added and then click "Add". This Special Application setting will then be added into the "Current Trigger-Port Table" below. If you find any errors before adding it and want to retype it again, just click "Clear" and the fields will be cleared. If you want to add a popular application, select one "Popular Application" and then click "Add".
Remove Special Application	If you want to remove some Special Application settings from the "Current Trigger-Port Table", select the Special Application settings you want to remove in the table and then click "Delete Selected". If you want to remove all Special Application settings from the table, just click the "Delete All" button. Clicking "Reset" will clear your current selections.

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

Example: Special Applications

 If you need to run applications that require multiple connections, then specify the port (outbound) normally associated with that application in the "Trigger Port" field. Then select the protocol type (TCP or UDP) and enter the public ports associated with the trigger port to open them up for inbound traffic.

Example:

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624	TCP	MSN Game Zone
2	6112	UDP	6112	UDP	Battle.net

In the example above, when a user triggers port 28800 (outbound) for MSN Game Zone then the router will allow incoming packets for ports 2300-2400 and 47624 to be directed to that user. **Note**: Only one LAN client can use a particular special application at a time.

2.4.4 UPnP

With UPnP, all PCs in your Intranet will discover/locate this router automatically. So you will not have to perform any configuration procedures for your PC and can access the Internet through this router easily.
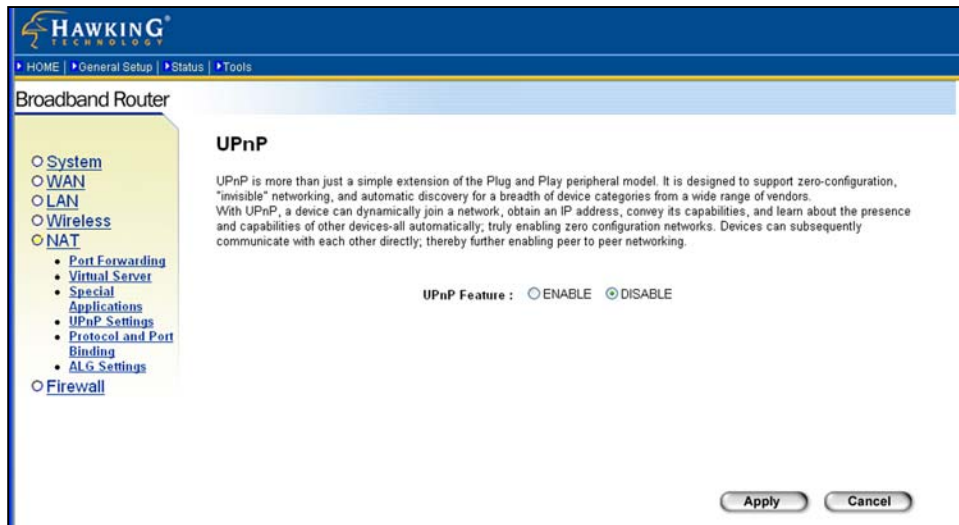
Figure 2.18

Parameters	Default	Description
UPnP Feature	Disable	You can Enable or Disable the UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover/locate this router automatically and access the Internet through this router without any configuration. The NAT Traversal function provided by UPnP can let applications that support UPnP smoothly connect to Internet sites without any incompatibility problem due to the NAPT port translation.

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

2.4.5 Protocol and Port Binding

Protocol and Port Binding let you manually bind an application to a WAN port. Only packets that match all the entered criteria will be bound to the assigned WAN port. You will have to fill all the items. The items that you leave blank will be ignored.
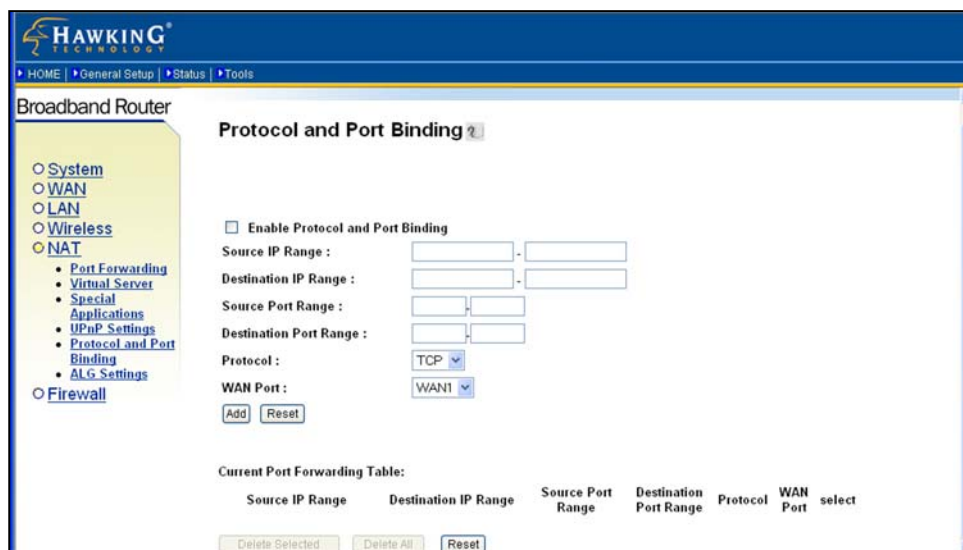

Figure 2.19

Parameters	Description
Enable Protocol & Port Binding	The "Protocol and Port Binding" function is disabled by default. You can select to enable the "Protocol and Port Binding" function.
Source IP Range	Only packets with this assigned source IP range will statically bind to the assigned WAN port.

Destination IP Range	Only packets with this assigned destination IP range will statically bind to the assigned WAN port.
Source Port Range	Only packets with this assigned source port range will statically bind to the assigned WAN port.
Destination Port Range	Only packets with this assigned destination port range will statically bind to the assigned WAN port.
Protocol	Only packets with this assigned protocol will statically bind to the assigned WAN port.
WAN Port	The WAN port that the packets matching this rule are statically bound to.
Add a Rule	Fill in the "Source IP Range", "Destination IP Range", "Source Port Range", "Destination Port Range", "Protocol" or "WAN Port" of the setting to be added and then click "Add". This rule of Protocol and Port Binding will then be added into the "Protocol and Port Binding Table" below. If you find any errors before adding it and want to retype it again, just click "Clear" and the fields will be cleared.
Remove a Rule	If you want to remove a rule from the "Protocol and Port Binding Table", select the rules you want to remove in the table and then click "Delete Selected". If you want to remove all rules from the table, just click the "Delete All" button. Clicking "Reset" will clear your current selections.

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

General Setup

H2BR4 Dual WAN 4-Port Firewall Router

2.4.6 ALG Settings

You can select applications that need "Application Layer Gateway" to support.
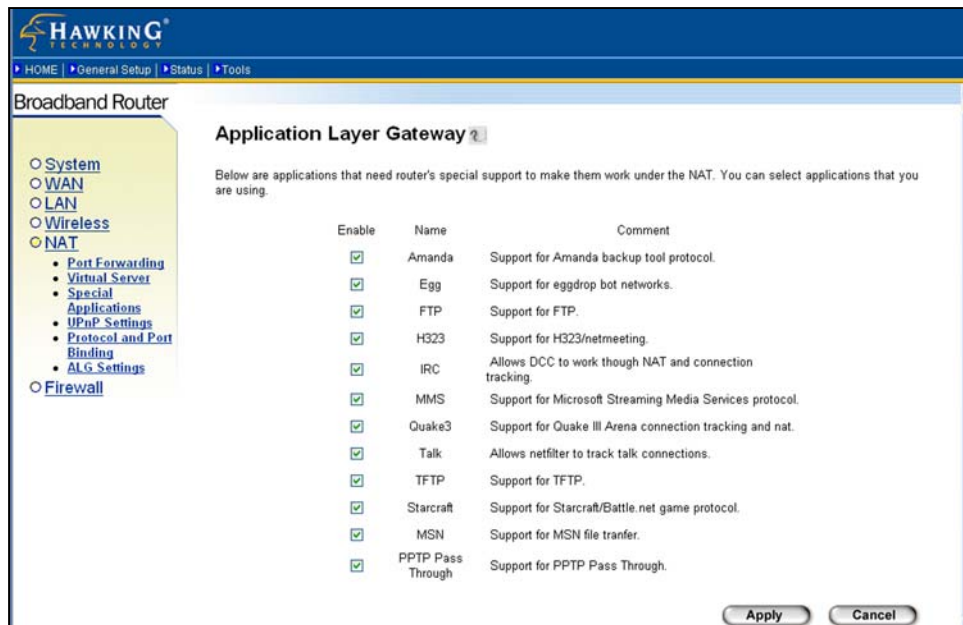
Figure 2.20

Parameters	Default	Description
Enable		You can enable the "Application Layer Gateway". Then, the router will let that application correctly pass though the NAT gateway.

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

2.4.7 Static Routing

This router provides a Static Routing function when NAT is disabled. With Static Routing, the router can forward packets according to your routing rules.

Note: The DMZ function of the firewall will not work if static routing is enabled.
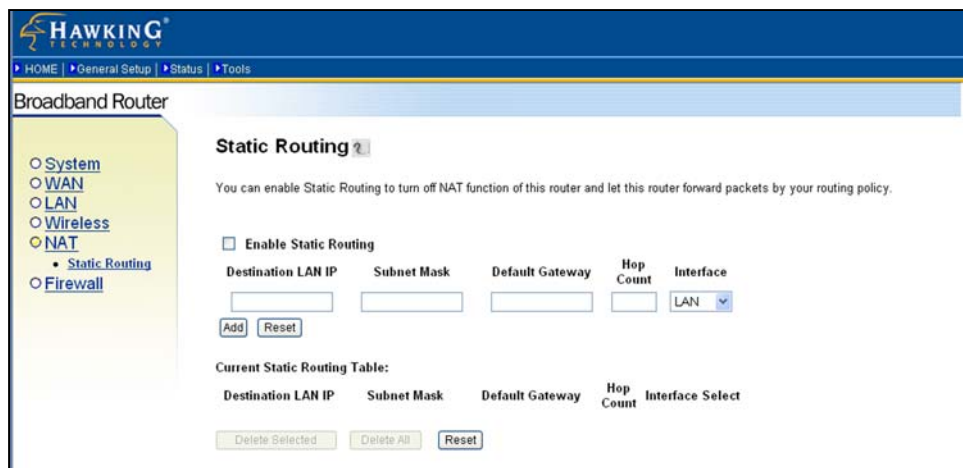
Figure 2.21

Parameter	Description
Enable Static Routing	The Static Routing function is disabled by default. You have to enable the Static Routing function before your routing rules take effect.
Destination LAN IP	The network address of the destination LAN.
Subnet Mask	The subnet mask of the destination LAN.
Default Gateway	The next stop gateway of the path toward the destination LAN. This is the IP address of the neighbor router that this router should communicate with on the path to the destination LAN.

Hop Count	The number of hops (routers) to pass through to reach the destination LAN.
Interface	The interface that goes to the next hop (router).
Add a Rule	Fill in the "Destination LAN IP", "Subnet Mask", "Default Gateway", "Hop Count" and "Interface" of the rule to be added and then click "Add". This rule for Static Routing will then be added into the "Static Routing Table" below. If you find any errors before adding it and want to retype it again, just click "Clear" and the fields will be cleared.
Remove a Rule	If you want to remove some routing rules from the "Static Routing Table", select the rules you want to remove in the table and then click "Delete Selected". If you want to remove all the rules from the table, just click the "Delete All" button. Clicking "Reset" will clear your current selections.

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

2.5 Firewall

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Note: To enable the Firewall settings select **Enable** and click **Apply**.

Figure 2.22

General Setup

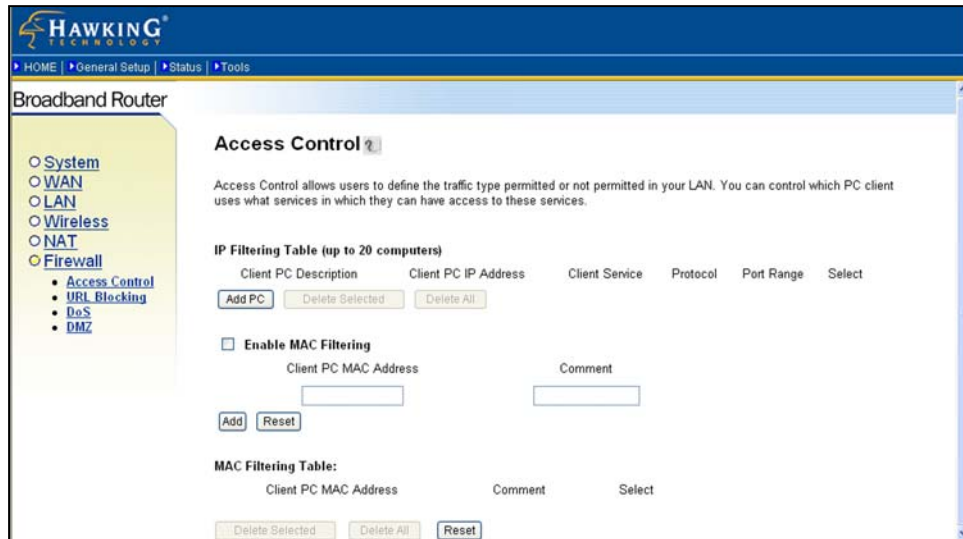H2BR4 Dual WAN 4-Port Firewall Router

Figure 2.23

Parameters	Description
2.5.1 Access Control	Access Control allows you to specify which hosts/users can have access to certain Internet applications.
2.5.2 URL Blocking	URL Blocking allows you to specify which URLs cannot be accessed by users.
2.5.3 DoS	The router's firewall can block common hacker attacks and can log the attack activities.
2.5.4 DMZ	The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN.

Click on one of the firewall selections and proceed to the manual's relevant sub-sections.

2.5.1 Access Control

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), you can change the relevant settings here. Access Control allows users to define the type of traffic permitted on your LAN. You can control which PC client can have access to these services.
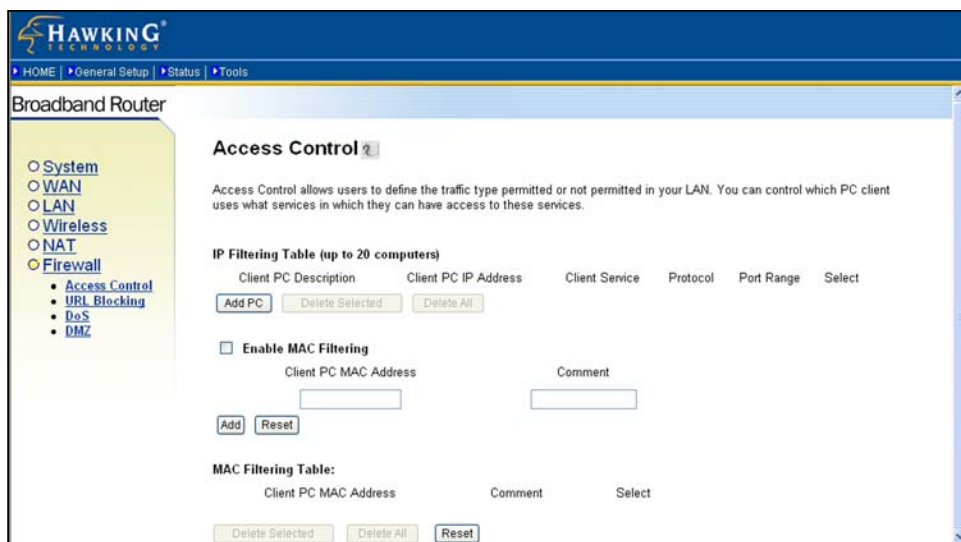

Figure 2.24

Parameters	Description
Filter client PCs by IP	Fill "IP Filtering Table" to filter PC clients by IP.
Add PC	You can click Add PC to add an access control rule for users by IP addresses.
Remove PC	If you want to remove some PC from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want remove all PCs from the table, just click the "Delete All" button.
Filter client PC by MAC address	Check "Enable MAC Filtering" to enable MAC Filtering.

| Add PC | Fill in "Client PC MAC Address" and "Comment" for the PC that will be allowed to access the Internet, and then click "Add". If you find any errors before adding it and want to retype it again, just click "Reset" and the fields will be cleared. |
| Remove PC | If you want to remove a PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button. If you want to clear the selection and re-select again, just click "Reset". |

You can now configure other advanced sections or start using the router (with the advanced settings in place).
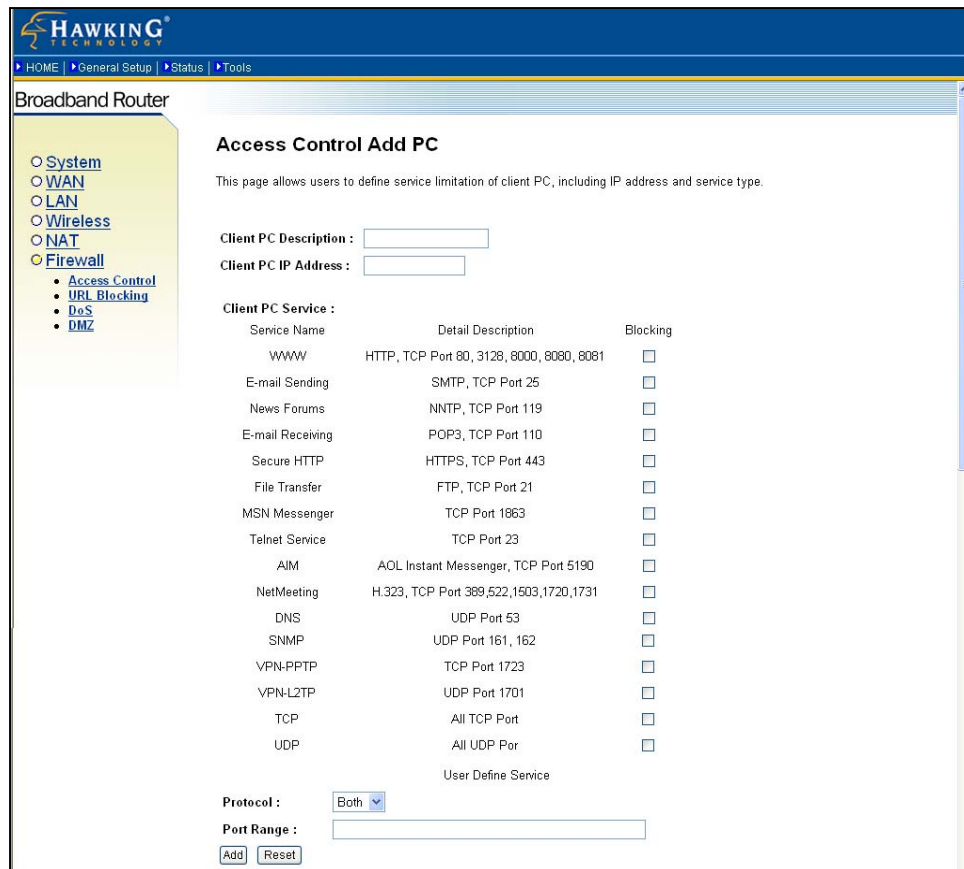

Figure 2.25

Add PC

Parameters	Description
Client PC Description	The description for this client PC rule.
Client PC IP Address	Enter the IP address that you wish to apply the Access Control rule to. This is the user's IP address for which you wish to setup an Access Control rule. **Note:** You need to give your LAN PC clients a fixed/static IP address for the Access Control rule to work properly.
Client PC Service	You can block the clients from accessing some Internet services by checking the services you want to block.
Protocol	This allows you to select UDP, TCP or both protocol types you want to block.
Port Range	You can assign up to five port ranges. The router will block clients from accessing Internet services that use these ports.
Apply Changes	Click "Apply Changes" to save the settings.
Reset	Click "Reset" to clear all fields.

Click **Apply Changes** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

Example: Access Control

In the example below, LAN client A can only access websites that use Port 80. However, LAN client B is able to access websites and any other service that uses ports between 80 and 999.
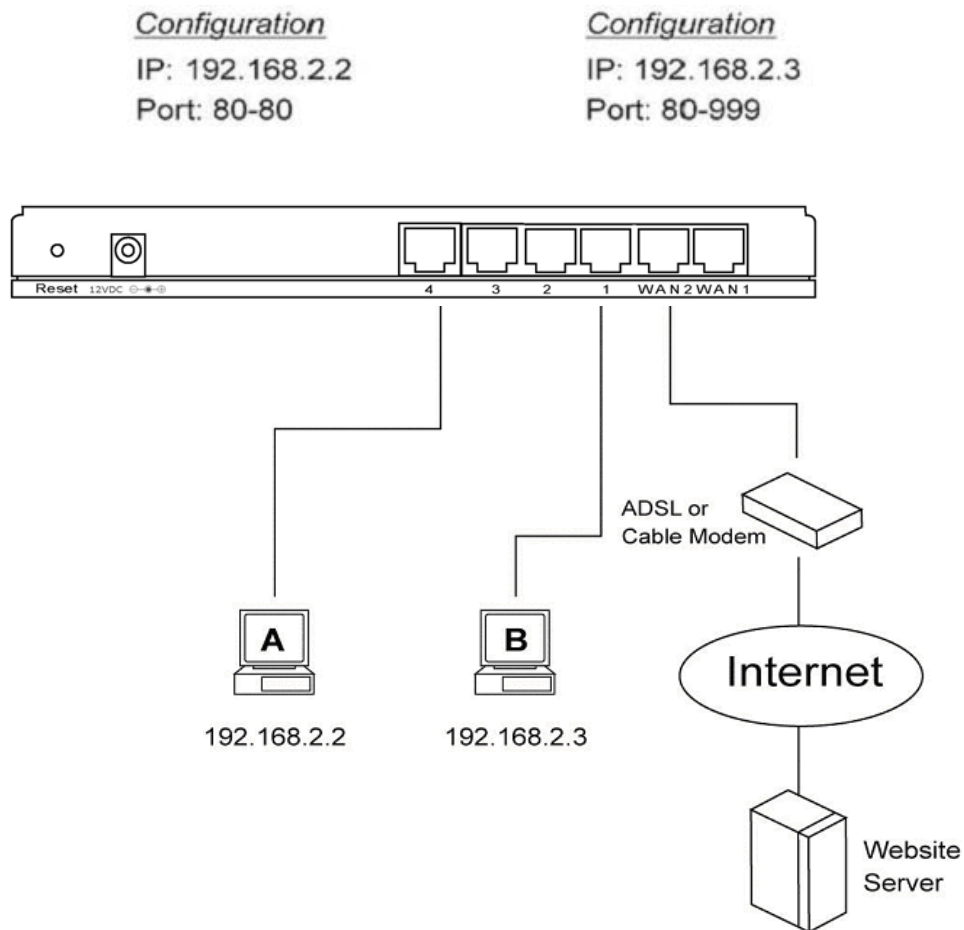

Figure 2.26

2.5.2 URL Blocking

You can block access to some Web sites from particular PCs by entering a full URL address or just a keyword of the web site.
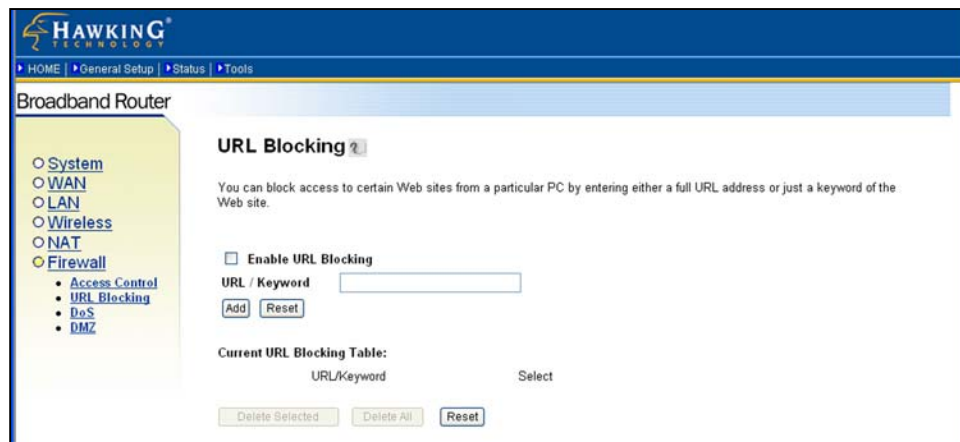

Figure 2.27

Parameters	Description
Enable URL Blocking	Enables/disables URL Blocking.
Add URL Keyword	Fill in the "URL/Keyword" and then click "Add". You can enter the full URL address or the keyword of the web site you want to block. If you find any errors before adding it and want to retype it again, just click "Reset" and the field will be cleared.
Remove URL Keyword	If you want to remove a URL keyword from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want to remove all URL keywords from the table, just click the "Delete All" button. If you want to clear the selection and re-select again, just click "Reset".

You can now configure other advanced sections or start using the router (with the advanced settings in place).

2.5.3 DoS (Denial of Service)

The Broadband router's firewall can block common hacker attacks, including Ping of Death, Discard Ping from WAN, Port Scan, and Sync Flood. If Internet attacks occur the router can log the events.
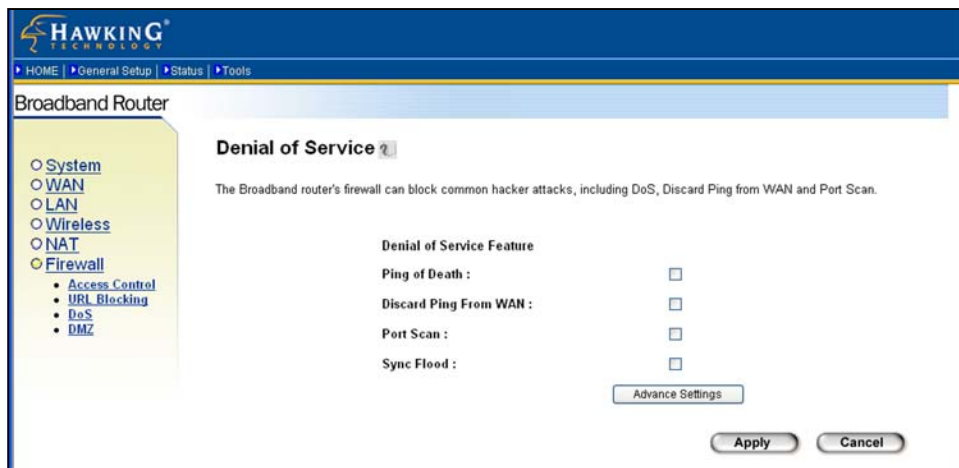

Figure 2.28
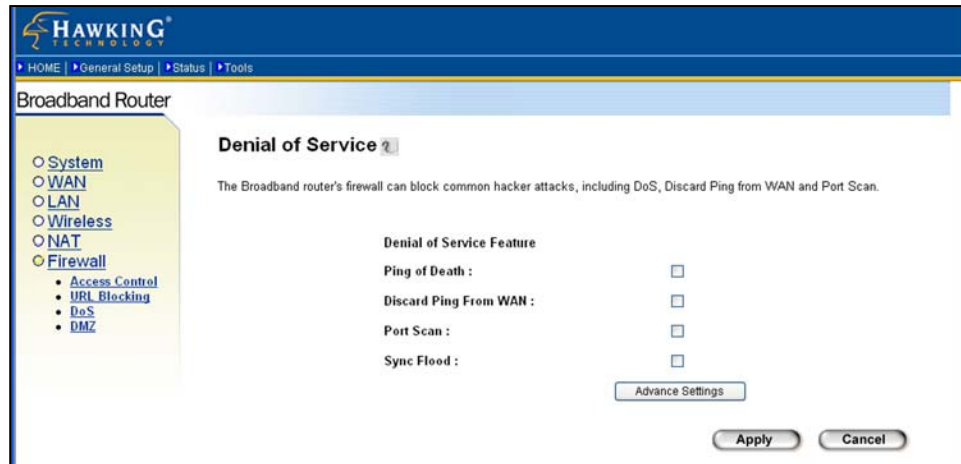
Figure 2.29

Parameters	Description
Intrusion Detection Features	
Ping of Death	Protections from Ping of Death attacks. From the Advanced Settings page, you can configure a threshold for the frequency of packet occurrence.
Discard Ping From WAN	The router's WAN port will not respond to any Ping requests
Port Scan	Protection from any Port Scan attacks. If you go to the Advanced Settings page, you can configure the pattern of Port Scan you want to prevent.
Sync Flood	Protection from any Sync Flood attacks. If you go to the Advanced Settings page, you can configure a threshold for the frequency of packet occurrence.

Click **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

2.5.4 DMZ

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

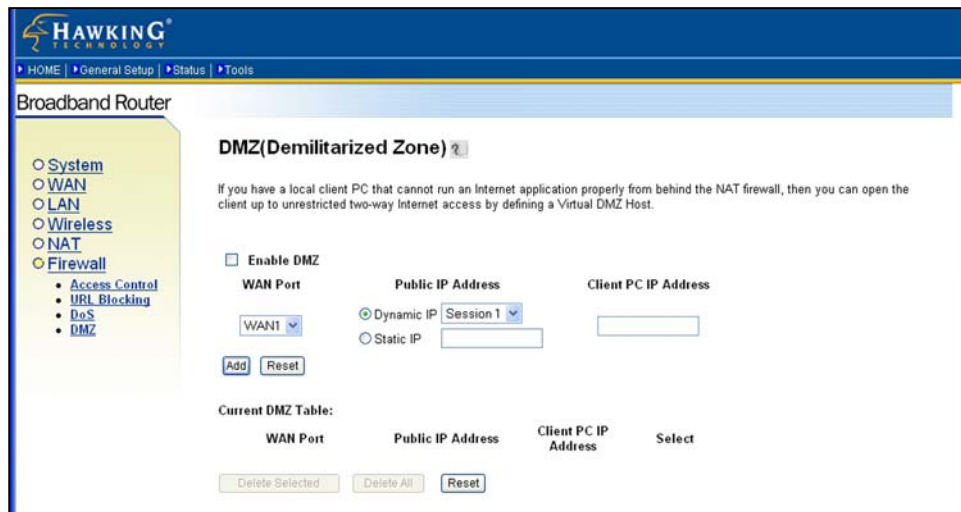Note: DMZ function works only when the NAT function is enabled.

Figure 2.30

Parameters	Description
Enable DMZ	Enables/disables DMZ. **Note**: If there is a conflict between the Virtual Server and the DMZ setting, then the Virtual Server function will have priority over the DMZ function.
WAN Port	The WAN port that the local client PC's IP address will bind to.
Public IP Address	The IP address of the WAN port or any other Public IP addresses given to you by your ISP. The WAN port may use dynamic IP or static IP given by your ISP. If your ISP gives you more than one dynamic IP address, you have to assign the session number that you want to apply.
Client PC IP Address	Input the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above. **Note:** You need to give your LAN PC clients a fixed/static IP address for the DMZ function to work properly.
Add DMZ	Fill in the "WAN Port", "Public IP Address" and "Client IP Address" of the DMZ to be added and then click "Add". This DMZ entry will then be added into the "DMZ Table" below. If you find any errors before adding it and want to retype it again, just click "Clear" and the fields will be cleared.
Remove DMZ	If you want to remove a DMZ from the "DMZ Table", select the DMZ entries you want to remove in the table and then click "Delete Selected". If you want to remove all DMZ entries from the table, just click the "Delete All" button. Clicking "Reset" will clear your current selections.

You can now configure other advanced sections or start using the router (with the advanced settings in place).

Status

The Status section allows you to monitor the current status of your router. You can use the Status page to monitor: the connection status of the router's WAN/LAN interfaces, the current firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.

Parameters	Description
3.1 Status and Information	Shows the router's system information
3.2 Internet Connection	View the router's current Internet connection status and other related information
3.3 Device Status	View the router's current setting status
3.4 System Log	View the router's system log
3.5 Security Log	View any attempts that have been made to illegally gain access to your network.
3.6 Active DHCP Client	View your LAN client's information that is currently linked to the router's DHCP server
3.7 Statistics	View the critical statistics

Select one of the above Status selections and proceed to the manual's relevant sub-section.

3.1 Status and Information

The Status and Information section allows you to view the router's system information.
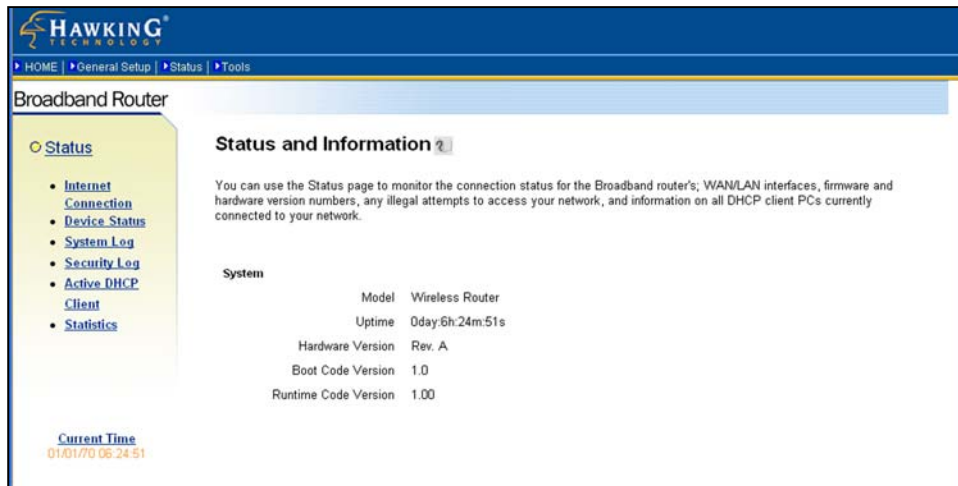

Figure 3.1

Parameters	Description
Information	You can see the router's system information, including the router's: Hardware version, Boot code Version, and Runtime code Version

3.2 Internet Connection

View the router's current Internet connection status and other related information.
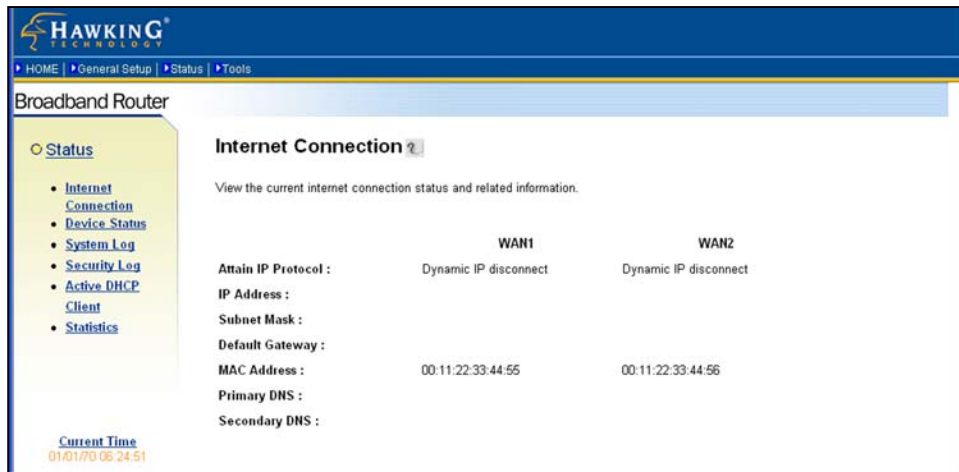

Figure 3.2

Parameters	Description
Internet Connection	This page displays whether the WAN ports are connected to **Cable/DSL** connections. It also displays the router's WAN port: **WAN IP** address, **Subnet Mask**, and ISP **Gateway** as well as the **Primary DNS** and **Secondary DNS** being used.

3.3 Device Status

View the router's current configuration settings. The Device Status displays the configuration settings you have configured in the **Quick Setup Wizard/General Setup** section.

Figure 3.3

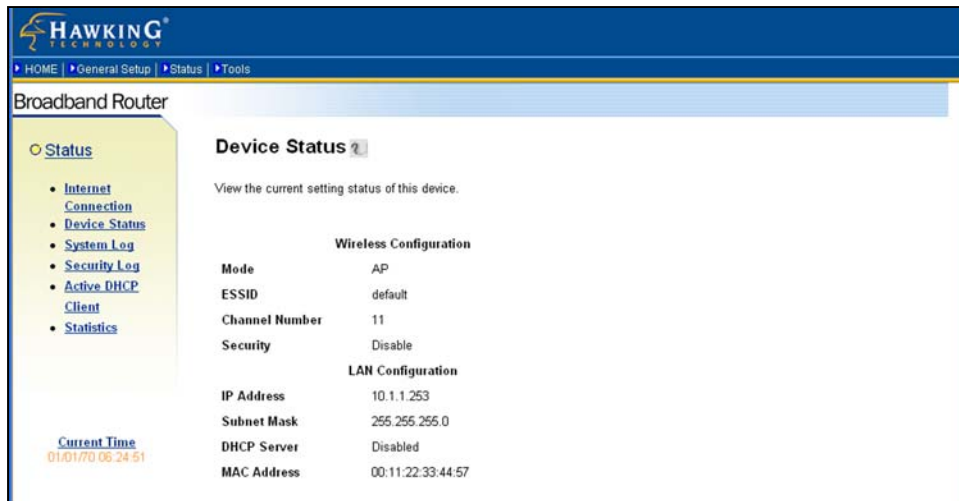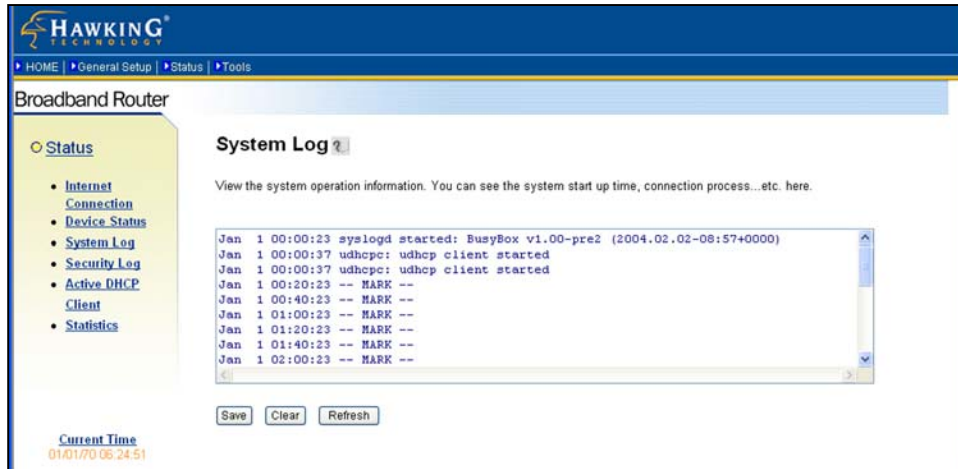| Parameters	Description
Device Status	This page shows the router's current device settings. This page displays the router LAN port's current LAN **IP Address** and **Subnet Mask**. It also shows whether the **DHCP Server** is enabled.

3.4 System Log

View the operation log of the system.

Figure 3.4

Parameters	Description
System Log	This page shows the current system log of the Broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved <**Save**> to a local file for further processing, or the system log can be cleared <**Clear**>, or it can be refreshed <**Refresh**> to get the most updated status. When the system is powered down, the system log will disappear if not saved to a local file.

3.5 Security Log

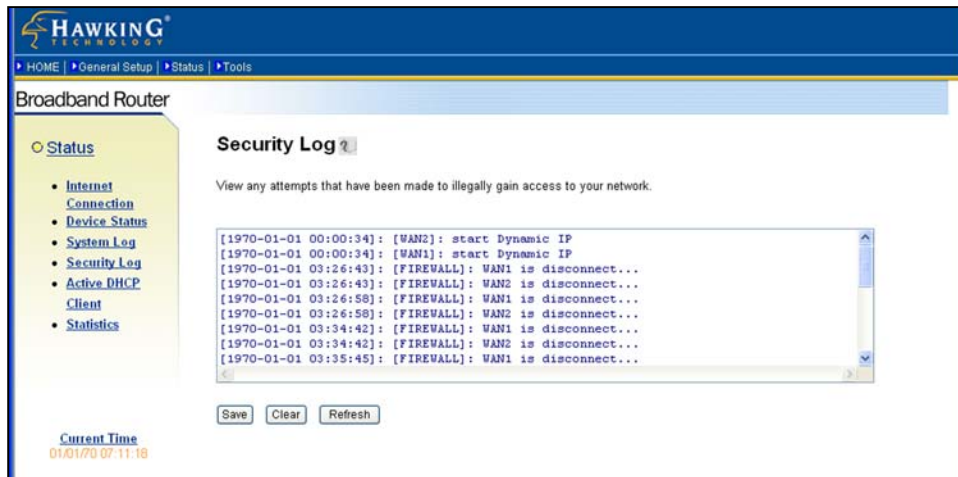View any attempts that have been made to illegally gain access to your network.

Figure 3.5

Parameters	Description
Security Log	This page shows the current security log of the Broadband router. It displays any illegal attempts to access your network. At the bottom of the page, the security log can be saved <**Save**> to a local file for further processing, or the security log can be cleared <**Clear**>, or it can be refreshed <**Refresh**> to get the most updated status. When the system is powered down, the security log will disappear if not saved to a local file.

3.6 Active DHCP Client

View your LAN client's information that is currently linked to the Broadband router's DHCP server
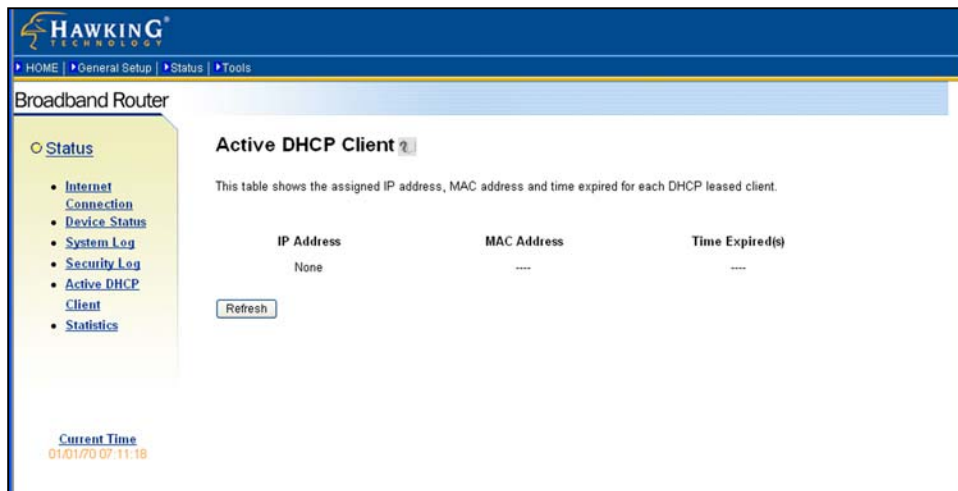

Figure 3.6

Parameters	Description
DHCP Client Log	This page shows all DHCP clients (LAN PCs) currently connected to your network. The "Active DHCP Client Table" displays the **IP** address and the **MAC** address and Time Expired for each LAN Client. Use the **Refresh** button to get the most updated status.

3.7 Statistics

View the statistics of packets sent and received over each WAN and LAN interface.
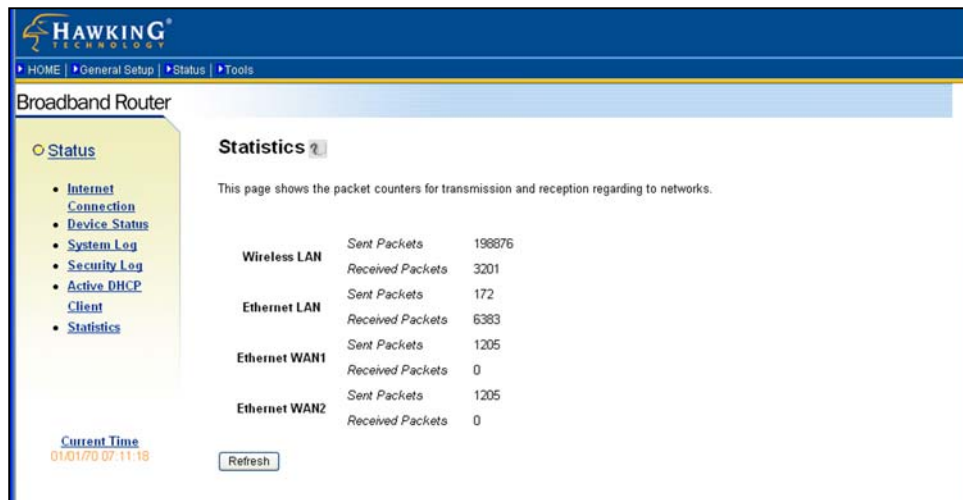
Figure 3.7

Parameters	Description
Statistics	Shows the counters for packets sent and received over the WAN and LAN interfaces.

Tools

This page includes the basic configuration tools, such as Configuration Tools (save or restore configuration settings), Firmware Upgrade (upgrade system firmware) and Reset.

Figure 4.1

Parameters	Description
4.1 Configuration Tools	You can save the router's current configuration, restore the router's saved configuration files and restore the router's factory default settings.
4.2 Firmware Upgrade	This page allows you to upgrade the router's firmware.
4.3 Reset	You can reset the router's system should any problems occur.

Select one of the above **Tool Settings** and proceed to the manual's relevant sub-section.

4.1 Configuration Tools

The Configuration Tools screen allows you to save (back up) the router's current configuration settings. Saving the configuration settings provides an added protection and convenience if problems occur with the router and you have to reset to the factory default. When you save (back up) the configuration settings, you can re-load the saved configuration into the router through the Restore selection. If more serious problems occur, you can use the Restore to Factory Defaults selection. This will set all configurations to their original default settings (i.e., when you first purchased the router).
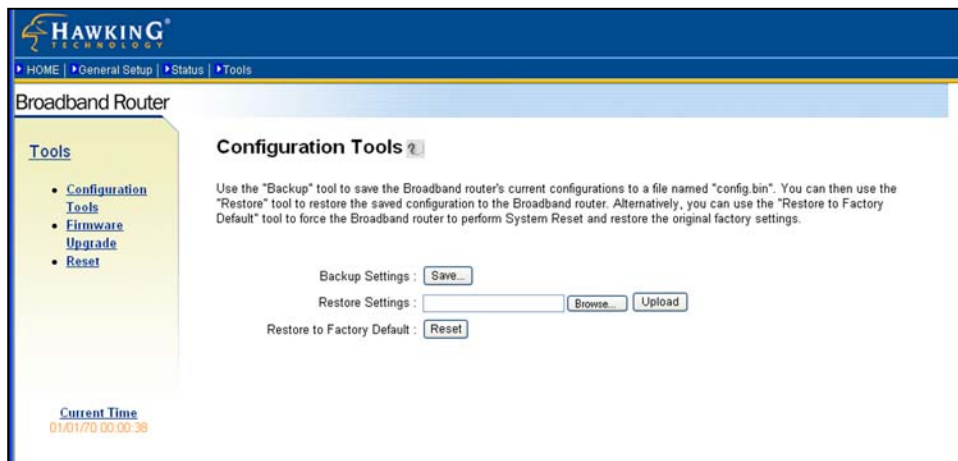

Figure 4.2

Parameters	Description
Configuration Tools	Use the "**Backup**" tool to save the router's current configuration to a file named "config.bin" on your PC. You can then use the "**Restore**" tool to restore the saved configuration to the router. Alternatively, you can use the "**Restore to Factory Defaults**" tool to force the router to perform a power reset and restore the original factory settings.

4.2 Firmware Upgrade
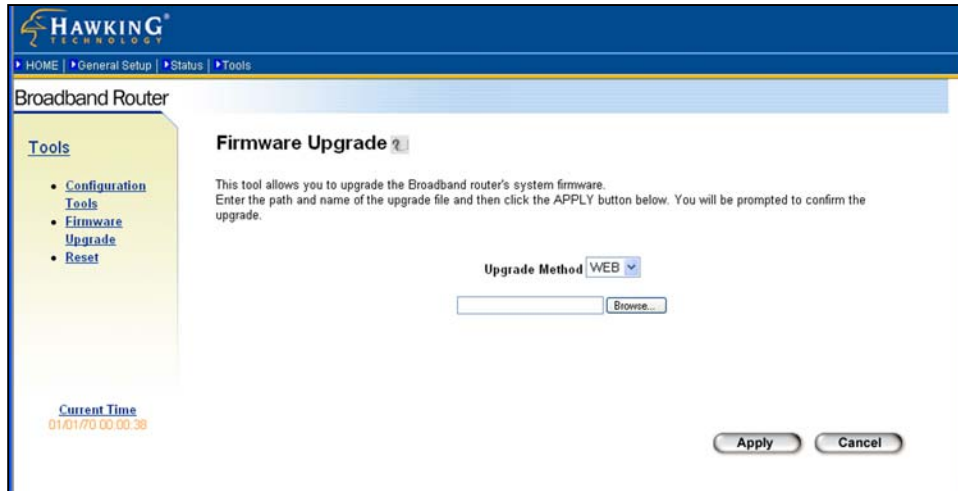
This page allows you to upgrade the router's firmware

Figure 4.3

Parameters	Description
Firmware Upgrade	This tool allows you to upgrade the router's system firmware. To upgrade your router's firmware, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you have selected the new firmware file, click **Apply** at the bottom of the screen to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete). Once the upgrade is completed you can start using the router.

4.3 Reset

You can reset the router's system if any problems occur. The reset function essentially re-boots your router's system.
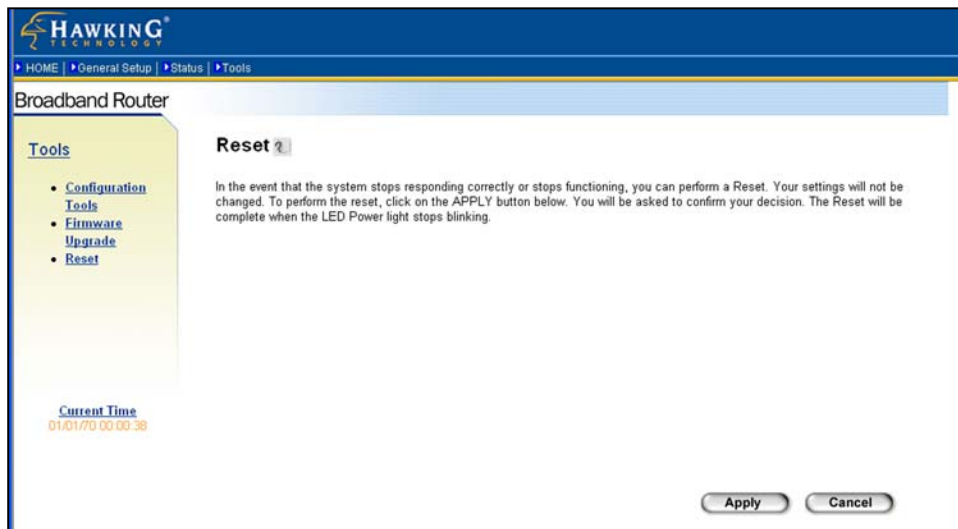

Figure 4.4

Parameters	Description
Reset	In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. **Your settings will not be changed**. To perform the reset, click on the **APPLY** button. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking. Once the reset process is complete you may start using the router again.

Appendix A

H2BR4 Dual WAN 4-Port Firewall Router

How to Manually Find Your PC's IP and MAC Addresses

1) In Windows, open the Command Prompt program.

2) Type **Ipconfig /all** and click **Enter**.

- Your PC's IP address is the one entitled **IP address** (192.168.1.77)
- The router's IP address is the one entitled **Default Gateway** (192.168.1.254)
- Your PC's MAC Address is the one entitled **Physical Address** (00-50-FC-FE-02-DB)

Bridge: A bridge is an intelligent, internetworking device that forwards or filters packets between different networks based on data link layer (MAC) address information.

Default Gateway (Router): Every non-router IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandrouter.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandrouter.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100/1000 million bits per second (Mbps).

Idle Timeout: Idle Timeout is designed so that if there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.
A network mask is also a 32-bit binary pattern, and consists of consecutive leading
1's followed by consecutive trailing 0's, such as
11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's.
When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form,
11011001.10110000.10010000.00000111, and if its network mask is,
11111111.11111111.11110000.00000000
It means the device's network address is
11011001.10110000.10010000.00000000, and its host ID is,
00000000.00000000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

NAT: Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the router's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network Clients (LAN PCs) use port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers.

Protocol: A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Router: A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocols. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to control/configure or monitor the device being managed.